4600 Series IP Telephone

Release 1.8
LAN Administrator's Guide

555-233-507
Issue 1.8
June 2003

Copyright 2003, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following website:
http://www.avaya.com/support

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya Web site:
http://www.avaya.com/support/
If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.
Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6

Federal Communications Commission Statement

Part 15:
Class B Statement:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that radio interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- **Reorient or relocate the receiving antenna.**
- **Increase the separation between the equipment and receiver.**
- **Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.**
- **Consult the dealer or an experienced radio/TV technician for help.**

DECLARATIONS OF CONFORMITY

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site:
http://www.avaya.com/support

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at:
http://www.part68.org/

by conducting a search using "Avaya" as manufacturer.

Trademarks

Avaya Communication Manager and MultiVantage are trademarks of Avaya, Inc. DEFINITY is a registered trademark of Avaya, Inc. Other trademarked references in this guide are the property of their respective owners.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site:
http://www.avaya.com/support/

To order copies of this and other documents:

Call: Avaya Publications Center

Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya Web site:
http://www.avaya.com/support/

4600 Series IP Telephone LAN Administrator's Guide

Table of Contents

1 Introduction

About This Guide 1-1
- Intended Audience 1-1

Document Organization 1-2
- Change History 1-2
- Terms Used in This Guide 1-3
- Conventions Used in This Guide 1-4

Online Documentation 1-4

Related Documents 1-5
- IETF Documents 1-6
- ITU Documents 1-8
- ISO/IEC, ANSI/IEEE Documents 1-8

Customer Support 1-8

2 Overview of Voice over IP (VoIP)

Introduction 2-1

Overview of Voice over IP 2-1
- Data and Voice Network Similarities 2-1
- Delay and Jitter 2-2
- Tandem Coding 2-2
- Voice Coding Standards 2-3
- H.323 Standard 2-3
- DHCP 2-3
- TFTP 2-3
- DNS 2-3
- NAT 2-4
- QoS 2-4

SNMP 2-4

Network Assessment 2-5
Suggestions for Installation and Configuration 2-6
- Reliability and Performance 2-6
- IP Address Lists and Station Number Portability 2-6
- Security 2-7

4600 Series IP Telephones 2-7
- Dual Connection Architecture 2-7
- Single Connection Architecture 2-7
- Registration and Authentication 2-8
- Software 2-8
- WAN Considerations 2-8
- DHCP and TFTP Servers 2-8

Initialization Process 2-9
- Step 1: Telephone to Network 2-9
- Step 2: DHCP Server to Telephone 2-9
- Step 3: Telephone and TFTP Server 2-9
- Step 4: Telephone and the Avaya Call Server 2-10

3 Requirements

Introduction 3-1

Hardware Requirements 3-1

Software Requirements 3-4

4 Server Administration

Introduction 4-1

Administering 4600 Series IP Telephones on Avaya Media Servers 4-4
- DEFINITY® Releases 9, 9.5, 10, and Avaya™ Communication Manager Software Release 1.1+ 4-4
- DEFINITY® Release 8.4 4-4

DHCP and TFTP 4-5

Software Checklist 4-5

Required Network Information 4-5

DHCP 4-6
- Choosing a DHCP Configuration 4-6
- DHCP Software Alternatives 4-7
- DHCP Generic Setup 4-7
- Windows NT® 4.0 DHCP Server 4-9
- Windows 2000® DHCP Server 4-14

TFTP 4-17
- TFTP Generic Setup 4-18
- Avaya TFTP (Suite Pro) 4-18

4600 Series IP Telephone Scripts and Application Files 4-19
- Contents of the Upgrade Script. 4-21
- Contents of the TFTP Settings File. 4-22

QoS 4-23
- IEEE 802.1D and 802.1Q 4-23
- DIFFSERV 4-24
- UDP Port Selection 4-25
- Network Audio Quality Display on 4600 Series IP Telephones 4-25
- RSVP and RTCP 4-27

VLAN Considerations 4-27

Administering Options for the 4600 Series IP Telephones 4-28
- DNS Addressing 4-31
- Customizing the Site-Specific Option Number (SSON) 4-31
- Entering Options via the Telephone Dialpad 4-32

Enhanced Local Dialing 4-32

Customizing the 4630/4630SW IP Telephone 4-33
- 4630/4630SW Backup/Restore. 4-36
- Call Log Archive 4-38

Customizing the 4620 IP Telephone 4-39

4620 Backup/Restore. 4-41

5 Troubleshooting Guidelines

Introduction 5-1

Error Conditions 5-1

The Reset Administrative Option 5-8
- Reset System Values 5-8
- Restart the Telephone 5-9

The View Administration Option 5-10

Error Messages 5-12

Appendix A: Avaya - 46xx IP Telephone MIB

Avaya - 46xx IP Telephone MIB. A-1

Appendix B: Creating Websites for the 4630/4630SW IP Telephone

Introduction B-1
General Background B-2
Browser Features and Behavior B-2
- Document Skeleton B-2
- Content-Based Style B-3
- Logical Style B-4
- Physical Style B-4
- Physical Spacing and Layout B-5
- Lists and Tables B-5
- Images B-7
- Links B-7
- Frames B-8
- Forms B-8
- Character Entities B-9
- Colors B-9
- Fonts B-9
- Cookies B-10

Design Guidelines B-10
- Fixed-Width Objects B-10
- Images B-11
- Frames B-11
- Fonts B-12
- Maintaining Context B-12
- User Interaction B-12

Appendix C: Creating Websites for the 4620 IP Telephone

Introduction C-1
General Background C-2
WML Document Skeleton C-2
Text Elements C-5
Text Formatting Tags C-5
Anchor Elements C-6
Image Elements C-7
Event Elements C-8
Task Elements C-12
Input Elements C-13
Variable Elements C-16

Character Entities. C-16
Colors and Fonts C-17
Wireless Telephony Applications (WTA) C-17
- Syntax Implementation C-19

Summary Of WML Tags And Attributes C-24

Appendix D: Administering the 4620 Thin Client Directory

Introduction D-1
Application Platform Requirements D-3
Installing the Thin Client Directory on the Server. D-3
- Pre-Installation Requirements (Apache/PHP). D-3
- Avaya-Provided Download Files. D-3
- Installing the Thin Client Directory D-4

4620 Web Application User Interface. D-7
- Generic User Interface Screen Characteristics. D-7
- Web Application Search Screen D-8
- Web Application Successful Search Screen. D-9
- Web Application Detail Screen D-10
- Web Application Directory Trouble Screen. D-11

Directory Database Administration Interface D-14
- Configuring the General Directory Application Administration Screen D-16
- Configuring the Directory Application Search Administration Screen. D-18
- Configuring the Directory Application Details Administration Screen. D-20
- Configuring the Directory Application Softkey Administration Screen. D-21

Index **IN-i**

Introduction

1

About This Guide

This guide provides a description of Voice over IP, describes how to administer the DHCP and TFTP servers and covers how to troubleshoot operational problems with the 4600 Series IP Telephones and the servers.

The 4600 Series IP Telephone product line is a supplement to Avaya's IP Solutions platform.

NOTE Unless otherwise indicated, references to "the DEFINITY® server" in this document also refer to the MultiVantage™ media servers.

Intended Audience

This document is intended for personnel administering the DHCP and TFTP servers to support the 4600 Series IP Telephones and those administering the Local Area Network (LAN) itself.

CAUTION:

Many of the products mentioned in this document are not supported by Avaya. Care should be taken to ensure there is adequate technical support available for the TFTP, DHCP, LDAP, and Web servers. If the servers are not functioning correctly, the 4600 Series IP Telephones may not operate correctly.

Document Organization

The guide contains the following sections:

Chapter 1, Introduction	Provides an overview of the 4600 Series IP Telephone LAN Administrator's document.
Chapter 2, Overview of Voice over IP (VoIP)	Describes VoIP and factors influencing its performance that must be considered when implementing this feature.
Chapter 3, Requirements	Describes the hardware and software requirements for Avaya's VoIP offering.
Chapter 4, Server Administration	Describes DHCP and TFTP administration for the 4600 Series IP Telephones.
Chapter 5, Troubleshooting Guidelines	Describes messages that may occur during the operation of the 4600 Series IP Telephones.
Appendix A, Avaya - 46xx IP Telephone MIB	Provides reference information about the MIB specification for the 46xx IP Telephones (4602/4602SW, 4606, 4612, 4620, 4624, and 4630/4630SW).
Appendix B, Creating Websites for the 4630/ 4630SW IP Telephone	Provides information on creating and customizing websites for viewing on the 4630/4630SW IP Telephone. Also describes the current capabilities and limitations of the 4630/4630SW's web browser.
Appendix C, Creating Websites for the 4620 IP Telephone	Provides information on creating and customizing websites for viewing on the 4620 IP Telephone. Also describes the current capabilities and limitations of the 4620's web browser.
Appendix D, Administering the 4620 Thin Client Directory	Provides information on administering an LDAP directory for the 4620 IP Telephone.

Change History

Issue 1.0	This document was issued for the first time in November 2000.
Issue 1.1	This version of the document, revised and issued in April 2001, supports through DEFINITY® Release 9.
Issue 1.5	This version of the document was revised in June, 2001 to support DEFINITY® Release 9.5.
Issue 1.6	This version of the document was revised to support DEFINITY® Release 10 and the 4630 IP Telephone.
Issue 1.7	This version of the document was revised in July, 2002 to support Avaya™ Communication Manager Release 1.1 and the 4602 and 4620 IP Telephones.
Issue 1.8	This is the current version of this document, revised to support Avaya™ Communication Manager Releases 1.2 and 1.3, as well as the 4602SW and 4630SW IP Telephones.

Terms Used in This Guide

802.1p 802.1Q	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1p, but the content of 802.1p is now incorporated in 802.1D.
ARP	Address Resolution Protocol, used to verify that the IP address provided by the DHCP server is not in use by another IP Telephone.
CELP	Code-excited linear-predictive; voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, type of TN799 circuit pack.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP addresses.
Gate-keeper	H.323 application that performs essential control, administrative, and managerial functions in the call server. Sometimes called CLAN, or TN799 in Avaya documents.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
LDAP	Lightweight Directory Access Protocol, an IETF standard for database organization and query exchange.
MAC	Media Access Control, ID of an endpoint.
NAPT	Network Address Port Translation.
NAT	Network Address Translation.
PHP	Hypertext Preprocessor, software used to assist in the format and display of web pages.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to a number of mechanisms intended to improve audio quality over packet-based networks.
RRQ	Read Request packet, a message sent from the 4600 Series IP Telephone to the TFTP server, requesting to download the upgrade script and the application file.
RSVP	Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
RTP	Real-time Transport Protocol, provides end-to-end services for real-time data (such as voice over IP).
TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to the IP Telephones.
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
VLAN	Virtual LAN.
WML	Wireless Markup Language, used by the 4620 web browser to communicate with WML servers.

Conventions Used in This Guide

This guide uses the following textual, symbolic, and typographic conventions to help you interpret information.

Symbolic Conventions

NOTE This symbol precedes additional information about a topic. This information is not required to run your system.

CAUTION:
This symbol is used to emphasize possible harm to software, possible loss of data, or possible service interruptions.

Typographic Conventions

This guide uses the following typographic conventions:

`command`	Words printed in this type are commands that you enter into your system.
device	Words printed in this type indicate parameters associated with a command for which you must substitute the appropriate value. For example, when entering the **`mount`** command, ***device*** must be replaced with the name of the drive that contains the installation disk.
Administrative	Words printed in bold type are menu or screen titles and labels, or items on menus and screens that you select to perform a task.
italics	Italic type indicates a document that contains additional information about a topic.
<Enter>	Words enclosed in angle brackets represent a single key that should be pressed. These include **<Ctrl>**, **<Enter>**, **<Esc>**, **<Insert>**, and **<Delete>**.

Online Documentation

The online documentation for the 4600 Series IP Telephones is located at the following URL:

http://www.avaya.com/support

Related Documents

- *DEFINITY® Documentation Release 8.4*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY switch with Release 8.4 software.

  This document is provided with the DEFINITY Release 8.4 product.

- *DEFINITY® Documentation Release 9*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY switch with Release 9 software.

  This document is provided with the DEFINITY Release 9 product.

- *DEFINITY® Documentation Release 10*

  This CD contains documentation that describes, among other things, how to administer a DEFINITY switch with Release 10 software.

  This document is provided with the DEFINITY Release 10 product.

- *Avaya™ Communication Manager Software Documentation Release 1.1*

  This document describes how to administer a switch with Avaya™ Communication Manager software.

  This document is provided with the Avaya™ Communication Manager Release 1.1 product.

- *Avaya™ Communication Manager Software Documentation Release 1.2*

  This document describes how to administer a switch with Avaya™ Communication Manager software.

  This document is provided with the Avaya™ Communication Manager Release 1.2 product.

- *Avaya™ Communication Manager Documentation Release 1.3*

  This document describes how to administer a switch with Avaya™ Communication Manager software.

  This document is provided with the Avaya™ Communication Manager Release 1.3 product.

- *Administration for Network Connectivity for Avaya™ Communication Manager Software (555-233-504)*

  This document describes how to implement Voice over IP (VoIP) applications for TCP/IP for DCS signaling, H.323 trunks, and private networks through Avaya™ Communication Manager software administration.

- *Administrator's Guide for Avaya™ Communication Manager Software (555-233-506)*

  This document provides an overall reference for planning, operating, and administering your Avaya™ Communication Manager solution.

The following documents are available on the web site listed above under Online Documentation:

- *4600 Series IP Telephones Safety Instructions (555-233-779)*

  This document contains important user safety instructions for the 4600 Series IP Telephones.

- *30A Switched Hub Set Up Quick Reference, Issue 2, July 2002 (Comcode 700234750; Document Number 555-236-700)*

  This document contains important safety and installation information for the 30A Switched Hub.

- *4600 Series IP Telephone Installation Guide (555-233-128)*

  This document describes how to install 4600 Series IP Telephones. It also provides troubleshooting guidelines for the 4600 Series IP Telephones.

- *4602/4602SW IP Telephone User's Guide (555-233-780)*

  This document provides detailed information about using the 4602/4602SW IP Telephones.

- *4606 IP Telephone User's Guide (555-233-765) (Int'l 555-233-769)*

  This document provides detailed information about using the 4606 IP Telephone.

- *4612 IP Telephone User's Guide (555-233-766) (Int'l 555-233-770)*

  This document provides detailed information about using the 4612 IP Telephone.

- *4620 IP Telephone User's Guide (555-233-781)*

  This document provides detailed information about using the 4620 IP Telephone.

- *4624 IP Telephone User's Guide (555-233-768) (Int'l 555-233-771)*

  This document provides detailed information about using the 4624 IP Telephone.

- *4630/4630SW IP Telephone User's Guide (555-233-764)*

  This document provides detailed information about using the 4630/4630SW IP Telephones.

IETF Documents

The following documents provide standards relevant to IP Telephony and are available for free from the IETF web site: http://www.ietf.org/rfc.html**.**

Requirements for Internet Hosts - Communication Layers, October 1989, by R. Braden (STD 3: RFC 1122)

Requirements for Internet Hosts - Application and Support, October 1989, by R. Braden (STD 3: RFC 1123)

Internet Protocol (IP), September 1981, by Information Sciences Institute (STD 5: RFC 791), as amended by *Internet Standard Subnetting Procedure*, August 1985, by J. Mogul and J. Postel (STD 5: RFC 950)

Broadcasting Internet Datagrams, October 1984, by J. Mogul (STD 5: RFC 919)

Broadcasting Internet Datagrams in the Presence of Subnets, October 1984, by J. Mogul (STD 5: RFC 922)

User Datagram Protocol (UDP), August 28, 1980, by J. Postel (STD 6: RFC 768)

Transmission Control Protocol (TCP), September 1981, by Information Sciences Institute (STD 7: RFC 793)

Domain Names - Concepts and Facilities (DNS), November, 1987, by P. Mockapetris (STD 13: RFC 1034)

Domain Names - Implementation and Specification (DNS), November 1987, by P. Mockapetris (STD 13: RFC 1035)

The TFTP Protocol (Revision 2), (TFTP), July 1992, by K. Sollins, (STD 33: RFC 1350:) as updated by *TFTP Option Extension*, May 1998, by G. Malkin and A. Harkin (RFC 2347)

An Ethernet Address Resolution Protocol (ARP), November 1982, by David C. Plummer (STD 37: RFC 826)

Dynamic Host Configuration Protocol (DHCP), March 1997, by R. Droms (RFC 2131)

DHCP Options and BOOTP Vendor Extensions, March 1997, by S. Alexander and R. Droms (RFC 2132)

RTP: A Transport Protocol for Real-Time Applications (RTP/RTCP), January 1996, by H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson (RFC 1889)

Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, *(DIFFSRV)*, December 1998, by K. Nichols, S. Blake, F. Baker and D. Black (RFC 2474)

Introduction to version 2 of the Internet-standard Network Management Framework (SNMPv2), April 1993, by J. Case, K. McCloghrie, M. Rose, and S. Waldbusser (RFC 1441)

Management Information Base for Network Management of TCP/IP Internets: MIB-II, March 1991, edited by K. McCloghrie and M. Rose (RFC 1213)

SNMPv2 Management Information Base for the Internet Protocol using SMIv2, November 1996, edited by K. McCloghrie (RFC 2011)

Structure of Management Information Version 2 (SMIv2), April 1999, edited by K. McCloghrie, D. Perkins, and J. Schoenwaelder (RFC 2578)

Resource ReSerVation Protocol VI, September 1997, by R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin (RFC 2205)

Lightweight Directory Access Protocol, March 1995, by M. Wahl, T. Howes, and S. Kille (RFC 1777)

Lightweight Directory Access Protocol (v3), December 1997, by M. Wahl, T. Howes, and S. Kille (RFC 2251)

Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, December 1997, by M. Wahl, Coulbeck, T. Howes, and S. Kitte (RFC 2252)

Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, December 1997, by M. Wahl, S. Kille, and T. Howes (RFC 2253)

ITU Documents

The following documents are available for a fee from the ITU web site: http://www.itu.int**.**

Recommendation G.711, Pulse Code Modulation (PCM) of Voice Frequencies, November 1988

Recommendation G.729, Coding of speech at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP), March 1996

Annex A to Recommendation G.729: Reduced complexity 8 kbit/s CS-ACELP speech codec, November 1996

Annex B to Recommendation G.729: A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70, November 1996

Recommendation H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communications systems, February 1998

Recommendation H.245, Control protocol for multimedia communication, February 1998

Recommendation H.323, Packet-based multimedia communications systems, February 1998

ISO/IEC, ANSI/IEEE Documents

The following documents are available for a fee from the ISO/IEC standards web site: http://www.iec.ch**.**

International Standard ISO/IEC 8802-2:1998 ANSI/IEEE Std 802.2, 1998 Edition, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks- Specific requirements- Part 2: Logical Link Control

ISO/IEC 15802-3: 1998 ANSI/IEEE Std 802.1D, 1998 Edition, Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Common specifications- Part 3: Media Access Control (MAC) Bridges

IEEE Std 802.1Q-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks

Customer Support

For support for your 4600 Series IP Telephones, call the Avaya support number provided to you by your Avaya representative or Avaya reseller.

Information about Avaya products can be obtained at the following URL:

http://www.avaya.com/support

Overview of Voice over IP (VoIP)

2

Introduction

This chapter describes the differences between data and voice networks, and the factors that influence the performance of VoIP. The installation and administration of 4600 Series IP Telephones on Avaya media servers, and the installation and configuration of DHCP and TFTP are addressed.

Overview of Voice over IP

The 4600 Series IP Telephones allow enterprises to use Voice over IP (that is, packet-switched networks) instead of telephony over the Public Switched Telephone Network (PSTN). However, the use of data networks for transmitting voice packets poses the problem that data networks were not designed for the specific qualities required by voice traffic.

Data and Voice Network Similarities

Data and voice networks share similar functions due to the nature of networking.

- **Signaling** is used to establish a connection between two endpoints.

  In a voice network, signaling helps identify who the calling party is trying to call and where the called party is on the network. Traditional telephony uses terminals with fixed addresses and establishes a fixed connection for the communication session between two such terminals, allocating fixed bandwidth resources for the duration of the call.

  IP communications constitute a connectionless network, having neither fixed addresses nor fixed connections.

- **Addressing**. Each terminal on a network must be identified by a unique address.

  In a voice network the unique address is a permanent attribute, based on international and national numbering plans, and/or local telephone company practices and internal customer-specific codes.

  In IP communications, dial plans track extension numbers assigned to terminals. No fixed connection path is needed.

- **Routing** is related to addressing and allows connections to be established between endpoints.

  Though these functions are common to data and voice networks, the implementations differ.

Delay and Jitter

Data traffic is generally short and comes in bursts. Data networks like the Internet were designed to manage these bursts of traffic from many sources on a first-come, first-served basis. Data packets are sent to multiple destinations, often without any attempt to keep them in a particular order.

Voice networks are designed for continuous transmission during a call. The traffic is not bursty, and the conversation uses a specific amount of bandwidth between the two ends for the duration of the call.

Several features of data networks are unsuitable for voice telephony:

- Data networks are designed to deliver data at the destination, but not necessarily within a certain time. This produces delay (latency). In data networks, delay tends to be variable. For voice messages, variable delay results in jitter, an audible chopiness in conversations.
- Variable routing also can result in loss of timing synchronization, so that packets are not received at the destination in the proper order.
- Data networks have a strong emphasis on error correction, resulting in repeated transmissions.

While data network concepts include prioritization of traffic types to give some forms of traffic greater reliability (for example, for interactive transactions), data requirements tend to not be as strict as most voice requirements.

Starting with Release 1.1, the 4600 Series IP Telephones include a dynamic jitter buffer. This feature automatically smooths jitter to improve audio quality.

Tandem Coding

Tandem coding (also called transcoding) refers to the conversion of a voice signal from analog to digital and back again. When calls are routed over multiple IP facilities, they may be subject to multiple transcodings. The multiple conversions between analog and digital coding result in a deterioration in the voice quality. Tandem coding should be avoided wherever possible in any compressed voice system (for example, by minimizing analog trunking on the PBX).

Voice Coding Standards

There are a number of voice coding standards. The Avaya 4600 Series IP Telephones offer the options described below:

- G.711, which describes the 64 kbps PCM voice coding technique. G.711-encoded voice is already in the correct format for digital voice delivery in the public phone network or through PBXs.
- G.729A and G.729B, which describe adaptive code-excited linear-predictive (CELP) compression that enables voice to be coded into 8 kbps streams.

H.323 Standard

Internal signaling provides connection control and call progress (status) information. The H.323 standard is used for internal signaling for IP packet voice networks. H.323 defines more than simply voice. It defines a complete multimedia network (voice, video, data), with everything from devices to protocols. The H.245 standard links all the entities within H.323 by negotiating facilities among participants and H.323 network elements.

The H.323 standard makes G.711 PCM compression the default form of compression. All other compression formats are optional.

DHCP

Dynamic Host Configuration Protocol (DHCP) allows a server to assign IP addresses and other parameters to devices such as the 4600 Series IP Telephones on an as-needed basis. This eliminates the need to configure each end station with a static IP address. The DHCP application also passes information to the 4600 Series IP Telephone, identifying the IP Addresses of the PBX and the TFTP server, and the paths to the upgrade script and the application file on the TFTP server. For further information, refer to DHCP and TFTP Servers, on page 2-8 and DHCP, on page 4-6.

TFTP

The Avaya 4600 IP Telephones get useful application information from the TFTP server. The telephones also upgrade themselves using files stored on the TFTP server. While the Avaya 4600 Series IP Telephones can operate without a TFTP server once software has been downloaded, some functionality can be lost if the TFTP server is not available when they are reset. For further information, refer to DHCP and TFTP Servers, on page 2-8 and TFTP, on page 4-17.

DNS

The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP Addresses. Release1.5 and later Avaya IP Telephones can use DNS to resolve names into IP Addresses. In DHCP and TFTP files, DNS names can be used wherever IP addresses were available as long as a valid DNS server is identified first (see DNS Addressing, on page 4-31).

NAT

A Network Address Translator is an application that can be administered between your network and the Internet. The NAT translates network layer IP addresses so your local intranet IP addresses can duplicate global, Internet addresses. A detailed discussion of NAT is beyond the scope of this document, but it should be noted that use of NAT can lead to problems affecting the consistency of addressing throughout your network. In Release 1.6 and earlier releases of the 4600 Series IP Telephones, NAT is **not** recommended for networks handling IP-based telephony traffic. As of Release 1.7, all 4600 Series IP Telephones support NAT interworking; hence, there are no problems with NAT and Release 1.7 of the 4600 Series IP Telephones. Note, however, that support for NAT does not imply support for Network Address Port Translation (NAPT). Specifically, the 4600 Series IP Telephones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the call server. The capability to have a direct Avaya IP Telephone-to-Avaya IP Telephone call with NAT (also called "NAT shuffling") requires Avaya™ Communication Manager Release 1.3 software. See the *Administration for Network Connectivity* document (listed in *Related Documents, on page 1-5*).

QoS

Quality of Service (QoS) is a term covering several initiatives to maximize the quality of the voice heard at both ends of a call that originates and/or terminates, on an IP-based telephone. These initiatives include various prioritization schemes to offer voice packets a larger or prioritized share of network resources. These schemes include standards such as IEEE's 802.1D and 802.1Q, the Internet Engineering Task Force's (IETF's) "Differentiated Services," RTP Control Protocol (RTCP), Resource ReSerVation Protocol (RSVP), and port-based priority schemes such as UDP port selection. Documentation for your LAN equipment will elaborate on the extent your network can support any or all of these initiatives. See Server Administration, on page 4-1, for some implications of QoS for the 4600 Series IP Telephones.

As of Release 1.7, both the 4620 and 4630 families of IP Telephones provided network audio quality information to the end user that may be of use to the LAN Administrator. As of Release 1.8, all 4600 Series IP Telephones provide some level of detail about network audio quality. For specific information, see Network Audio Quality Display on 4600 Series IP Telephones, on page 4-25.

SNMP

Simple Network Management Protocol (SNMP) is a family of standards-based protocols and procedures to allow vendor-independent data network management. Using a simple set of protocol commands, an SNMP-compliant device stores information in standard format in one or more Management Information Bases (MIBs). In general, devices support the standards-specific MIB termed MIB-II. In addition, devices may define one or more "custom MIBs" that contain information about the specifics of the device.

As of Release 1.1, the 4600 Series IP Telephones are fully compatible with SNMPv2c (a later version of SNMP) and with Structure of Management Information Version 2 (SMIv2), although the telephones will respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that the telephones respond to queries directed either at the MIB-II or the Custom MIB. The 4600 Series IP Telephone Custom MIB is read-only (values therein cannot be changed externally via network management tools). Similarly, although the 4600 Series IP Telephone’s MIB-II has read/write permissions in accordance with the standard, any writes to MIB-II are ignored to improve security.

More information about SNMP and MIBs can be found in the IETF references listed in Related Documents, on page 1-5. Appendix A, Avaya - 46xx IP Telephone MIB in this LAN Administration Guide provides information about the Custom MIB, which is available for download in *.txt format on the Avaya support website.

Network Assessment

The current technology allows optimum network configurations to deliver VoIP with perceived voice quality close to that of the Public Switched Telephone Network (PSTN). Not every network is able to take advantage of packet voice transmissions. Some data networks have insufficient residual capacity for even compressed voice traffic. In addition, the usual approach to developing data networks by integrating products from many vendors makes it necessary to test the components for compatibility with Voice over IP traffic.

It is assumed that your organization has performed a network assessment (with or without the assistance of Avaya) before attempting to install Voice over IP, in order to have a high degree of confidence that the existing data network has the capacity to carry voice packet traffic and is compatible with the required technology.

A network assessment would include a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.

The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, DHCP, TFTP, and jitter buffers in H.323 applications.

It is important to distinguish between compliance with the minimal VoIP standards and support for QoS, which is needed to run VoIP on your configuration.

Suggestions for Installation and Configuration

Reliability and Performance

There is a cost/performance trade-off associated with Voice over IP. Greater reliability and improved performance can be obtained through server redundancy and components with higher bandwidth capabilities.

The reliability and performance of the traditional PBX systems have been very high. Although much of the LAN is outside of the control of the PBX, there are several points to consider which enhance the reliability and performance of the IP Telephone network.

All 4600 Series IP Telephones support the tools "ping" and "traceroute." These are standard LAN/WAN tools for identifying whether two points on a network can communicate with each other, and what path a sample communication takes as it traverses the network from one point to the other. All 4600 Series IP Telephones will respond appropriately to a ping or a traceroute message sent from the DEFINITY® or MultiVantage™ switch or any other source on your network, although these telephones will not, in general, initiate a ping or traceroute. Release 1.6 of the 4600 Series IP Telephones introduced "remote ping" and "remote traceroute" support. The switch can instruct such a 4600 Series IP Telephone to initiate a ping or a traceroute to a specified IP address. The telephone carries out that instruction and sends a message to the switch informing it of the results. See your DEFINITY® or MultiVantage™ Administration documentation for more details.

As of Release 1.8, if applicable, 4600 Series IP Telephones test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by pinging the router with a tagged frame (see VLAN Considerations, on page 4-27). If your LAN environment includes Virtual LANs (VLANs), your router will need to respond to pings to VLAN tagging to work properly.

IP Address Lists and Station Number Portability

Release 1.5 of the 4600 Series Telephones provided the capability to specify IP address lists (in either dotted decimal or DNS format) for key elements of the network, rather than merely one address for each. Specifically, you can specify up to 127 total characters in each list of the following: router/gateways, TFTP servers, and the call server. When the 4600 telephone is powered up or is rebooted, it attempts to establish communication with these various network elements in turn, starting with the first address on the respective list. If the communication is denied or times out, the telephone proceeds to the next address on the appropriate list and tries that one. The telephone does not report failure unless all the addresses on a given list have failed.

Obviously, this capability can significantly improve the reliability of IP telephony by maximizing the likelihood of the telephone communicating with backup equipment if the primary equipment is down or inaccessible (say, perhaps due to a limited network outage).

However, this capability also has the advantage of making station number portability easier. Assume a situation where the company has multiple locations (for example, London and New York), all sharing a corporate IP network. Users want to take their telephones from their offices in London and bring them to New York. When users power up their telephones in the new location, the local DHCP server will generally route them to the local switch, which denies service because it knows nothing about these new users. However, with proper administration of the local DHCP server, the telephone knows to try a second call server IP address, this one in London. The user can then be automatically registered with the London switch.

Chapter 4, Server Administration contains details on administration of DCHP servers for lists of alternate call servers, router/gateways, and TFTP servers. For specific information, see DNS Addressing, on page 4-31.

Security

In VoIP, physical wire is replaced with an IP connection. The connection is more mobile. Unauthorized relocation of the IP telephone allows unauthorized users to send and receive calls as the valid owner. For further details on toll fraud, refer to the DEFINITY® or MultiVantage™ documents in Related Documents, on page 1-5.

Any equipment on a data network, including a 4600 Series IP Telephone, can be the target of a Denial of Service attack. Typically, such an attack consists of flooding the network with so many messages that the equipment either spends so much time processing them that it cannot process legitimate tasks, or the equipment overloads and fails. Although the 4600 Series IP Telephones cannot guarantee resistance to all Denial of Service attacks, each Release has increasing checks and protections to resist such attacks while maintaining appropriate service to legitimate users.

4600 Series IP Telephones

Dual Connection Architecture

Releases 1.0 and 1.1 of the 4600 Series IP Telephones use dual connection architecture to communicate with the DEFINITY® switch. In the dual connection architecture, two station extensions must be administered for each telephone.

Single Connection Architecture

Release 1.5 and subsequent releases of the 4600 Series IP Telephones use single connection architecture to communicate with the Avaya media server switch. In the single connection architecture, only one station extension must be administered for each telephone.

Registration and Authentication

The Avaya media server switch supports registering and authenticating 4600 Series IP Telephones using the extension and password. For further information, see Related Documents, on page 1-5.

Software

As shipped from the factory, the 4600 Series IP Telephones may not contain sufficient software for registration and operation. When the phone is first plugged in, a software download from a TFTP server is initiated. This gives the phone its proper functionality.

For downloads of software upgrades, the PBX provides the capability for a remote restart of the 4600 Series IP Telephone. As a consequence of restarting, the phone automatically restarts reboot procedures. If new software is available, a download will result.

WAN Considerations

QoS is harder on a WAN than a LAN. A LAN assumes no bandwidth concerns. A WAN assumes a finite amount of bandwidth. Therefore, QoS considerations are more significant when the IP telephony environment includes a WAN. In addition, there are administrative and hardware compatibility issues unique to WANs. WAN administration is beyond the scope of this document.

DHCP and TFTP Servers

The DHCP server provides the following information to the 4600 Series IP Telephone:

- IP Address of the 4600 Series IP Telephone
- IP Address of the TN799 board on the Avaya Call Server.
- IP Address of the TFTP server
- The subnet mask
- IP Address of the router
- DNS Server IP Address

You should administer the LAN so that every IP Telephone can access a DHCP server with the above information.

The IP Telephone will not function without an IP address. The failure of a DHCP server at boot time will leave all the affected voice terminals unusable. It is possible for the user to manually assign an IP address to an IP Telephone, but when the DHCP server finally returns, the telephone will never look for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process. It is therefore **strongly recommended** that a DHCP server be available when the IP Telephone reboots.

A minimum of two DHCP servers are recommended for reliability.

The TFTP server provides the 4600 Series IP Telephone with a script file and, if appropriate, new or updated application software (see Step 3: Telephone and TFTP Server, on page 2-9 under Initialization Process, on page 2-9). In addition, you can edit an associated settings file to customize telephone parameters for your specific environment (see Administering Options for the 4600 Series IP Telephones, on page 4-28).

Initialization Process

The following is a high-level description of the information exchanged when the telephone is initializing and registering. This description, which assumes all equipment is properly administered ahead of time, may be helpful in explaining how the 4600 Series IP Telephones relate to the routers and servers in your network.

Step 1: Telephone to Network

The telephone is appropriately installed and powered. After a short initialization process, the telephone identifies the LAN speed and sends a message out into the network, identifying itself and requesting further information. A router in the network receives this message and relays it to the appropriate DHCP server.

Step 2: DHCP Server to Telephone

The DHCP server provides information to the telephone, as described in DHCP and TFTP Servers, on page 2-8. Among other data passed to the telephone is the IP address of the TFTP server, which is crucial for the next step.

Step 3: Telephone and TFTP Server

The telephone queries the TFTP server, which transmits a script file to the telephone. This script file, at a minimum, tells the telephone which application file the telephone should be using (the application file is the software that has the telephony functionality, and can be easily updated for future enhancements).

The telephone uses the script file to determine if it has the proper application file. A newly-installed telephone may have no application file, and hence may not have the proper one. A previously-installed telephone may or may not have the proper application file. In any event, if the telephone determines it does not have the application file the script file says the telephone should have, the telephone requests a download of the proper application file from the TFTP server. The TFTP server then downloads the file and conducts some checks to ensure the file was downloaded properly. If the telephone determines it already has the proper file, it proceeds to the next step without downloading the application file again.

After the application file has been checked and loaded, if appropriate, the 4600 Series IP Telephone also uses the script file to determine if there is a settings file containing options you have administered for any or all of the 4600 Series IP Telephones in your network. For more information about this settings file, see Administering Options for the 4600 Series IP Telephones, on page 4-28.

Step 4: Telephone and the Avaya Call Server

In this step, the telephone and the PBX exchange a series of messages which cause the display on the telephone to prompt the user. For a new installation, the user must enter the telephone's extension and the call server password. For a restart of an existing installation, this information is already stored on the telephone, but the user may have to confirm the information. The telephone and the switch exchange more messaging, with the expected result that the telephone is appropriately registered on the switch.

More details about the installation process are available in the *4600 Series IP Telephone Installation Manual* and in Chapter 3, Requirements, on page 3-1 of this document.

Requirements

3

Introduction

The 4600 Series IP Telephones use Internet Protocol (IP) technology with Ethernet line interfaces. The IP telephones supplement the existing Avaya IP Solutions platform. This feature provides the user with the capability to natively administer and maintain the new 4600 Series IP Telephones.

The 4600 Series IP Telephones provide support for DHCP and TFTP over IPv4/UDP which enhance the administration and servicing of the phones. These phones use DHCP to obtain dynamic IP addresses and TFTP to download new versions of software for the phones.

The 4600 Series IP Telephones provide the ability to have one connection on the desktop for both the telephone set and the PC using the telephone's built-in hub.

Hardware Requirements

Before plugging in the 4600 Series IP Telephone, verify that all of the following requirements have been met. Failure to do so will prevent the telephone from working and may have a negative impact on your network.

The following hardware is required for 4600 Series IP Telephones to work properly:

Switch software release	Telephone model(s)	Telephone software release
DEFINITY® R8.4	4612, 4624	R1.0
DEFINITY® R9.0	4612,4624	R1.1
DEFINITY® R9.5 or later	4606, 4612, 4624	R1.5 or later
DEFINITY® R10	4630 or 4630SW	R1.60 or later
Avaya™ Communication Manager Software 1.1 or later	4620	R1.70 or later
Avaya™ Communication Manager Software 1.1 or later	4602 or 4602SW	R1.61 or later

NOTE The recommended configuration is the latest PBX software and the latest IP Telephone firmware. In the event your site does not have the latest PBX software, follow the recommendations in the table immediately below:

Call Server Release	Avaya IP Telephone	IP Telephone Release	Notes
Avaya™ Communication Manager 1.3+	All Telephones	R1.8+	Use the latest release.
Avaya™ Communication Manager 1.1, Avaya™ Communication Manager 1.2	All Telephones *except* 4630	R1.8+	Use the latest release.
R10, Avaya™ Communication Manager 1.1, Avaya™ Communication Manager 1.2	4630	R1.74	Upgrade to Avaya™ Communication Manager Release 1.3 or later before installing R1.8 on 4630 telephones.
R10	4606, 4612, 4624	R1.8+	The 4602 and 4620 are not supported.
R9.5	4606, 4612, 4624	R1.8+	The 4620, 4602, and 4630 are not supported. R1.5 is the minimum 4600 IP Telephone vintage.
R9	4612, 4624	R1.1	R1.1 is the only supported 4600 IP Telephone vintage.
R8.4	4612, 4624	R1.0	R1.0 is the only supported 4600 IP Telephone vintage.

Hardware Requirements, continued:

- Be sure the appropriate circuit pack(s) are administered on your call server. See the call server's hardware guide for more detail.
- A Category 5e LAN. If the telephones are to be powered from the LAN, the power supply must be designed to the IEEE 802.3af standard for LAN powering.
- Electrical power provided to each phone by one of the following two sources:
  - A Telephone Power Module (DC power jack) (must be ordered separately, except for the 4630, which does come with its own power brick).
  - IEEE 802.3af, if the LAN supports this powering scheme (note that the 4630 **cannot** be powered this way, but the 4630SW **can** be powered this way).
- Verify that the 4600 Series IP Telephone package includes the following components:
  - 1 telephone set.
  - 1 AB1C handset.
  - 1 H4DU 9-foot long (when extended) 4-conductor coiled handset cord, plugged into the telephone and the handset.
  - 1 Category 5e modular line cord for the connection between the IP Telephone and the Ethernet wall plug.
  - Non-system-specific safety and installation documentation.
  - Power brick (4630 only).
  - Stylus (4630/4630SW IP Telephones only).
- You may need a Category 5e modular line cord for the connection from the 4600 Series IP Telephone to the PC.

Refer to the *4600 Series IP Telephone Installation Guide*.

The IP telephones work the same on all DEFINITY®/MultiVantage™ platforms.

Software Requirements

The following software is required for 4600 Series IP Telephones to work properly.

- The DHCP server and application should be installed and properly administered, as described in DHCP, on page 4-6.

  WARNING:

  A DHCP server is not mandatory, but static addressing is necessary when a DHCP server is unavailable.
  Due to the difficulties associated with static addressing, it is very strongly recommended that a DHCP server be installed and that static addressing be avoided.

- The TFTP server and application must be installed and properly administered, as described in TFTP, on page 4-17.

  WARNING:

  A TFTP server does not need to be available for the Avaya IP Telephones to operate. The Avaya IP Telephones obtain important information from the script files on the TFTP server and depend on the TFTP file for software upgrades. If the TFTP server is not available when the Avaya IP Telephones reset, they will register with the call server and operate. Some features may not be available, and restoring those features will require resetting the Avaya IP Telephone(s) when the TFTP server is available.

- For 4630 and 4630SW IP Telephone environments, if users are to have access to LDAP directories or corporate Websites, the appropriate servers must be in place, and the 4630/ 4630SW telephones must be appropriately administered in accordance with Server Administration, on page 4-1.

  WARNING:

  *4630 IP Telephone Release 1.72 introduced significant software architecture changes. Thus, unlike most 4600 Series IP Telephones software releases, 4630 IP Telephone Release 1.72 and later **cannot** be downgraded to a release earlier than 1.72. Attempting to do so will render the 4630 (and 4630SW if Release 1.8 or greater) set inoperable. In addition, if you are upgrading a 4630 from a release prior to Release 1.61, you must first upgrade to Release 1.61, and then upgrade to the newer Release. You **cannot** upgrade directly from a pre-1.61 Release to a post-1.61 Release for the 4630.*

- For 4620 IP Telephone environments, if users are to have access to LDAP directories or corporate WML websites, the appropriate servers must be in place, the LDAP Directory Application software must be downloaded from the Avaya support website, and the 4620 telephones must be appropriately administered in accordance with Server Administration, on page 4-1.

Ensure that all required parameters are configured correctly. For Avaya media server information, see your administration documentation. For the DHCP and TFTP servers, see Server Administration, on page 4-1.

Server Administration

4

Introduction

When a 4600 Series IP Telephone is plugged in and powered, it automatically negotiates with its associated LAN to determine the Ethernet speed. From that point on, the actions taken by the phone depend in large part on the administration of the network before the phone is installed, and on the actions taken, if any, by the installer. This chapter discusses in detail the parameters and other data the telephone needs to operate and the alternatives for delivering that information to the telephone, where appropriate. Recommendations and specifications on which alternative(s) to choose for which parameter(s) are also provided.

The parameters under which the phone needs to operate are summarized as follows:

- Telephone Administration on the Call Server.
- IP address management for the telephone.
- Tagging Control and VLAN administration for the telephone, if appropriate.
- Quality of Service (QOS) administration for the telephone, if appropriate.
- Site-specific Option Number (SSON) setting of DHCP servers, if appropriate.
- Interface administration for the telephone, if appropriate.
- Application-specific administration for the telephone, if appropriate (for example, Directory- or Web-specific information required for these optional 4630/4630SW applications).

The delivery mechanisms are:

- Maintaining the information on the Avaya media server.
- Manually entering the information via the telephone dialpad.
- Administering the DHCP Server.
- Editing the settings file on the TFTP Server.

These parameters can be administered in a variety of ways, as indicated in Table 4-1, below. Note that not all parameters can be administered on all delivery mechanisms.

Table 4-1. Administration Alternatives and Options for 4600 Series IP Telephones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Call Server	Administering 4600 Series IP Telephones on Avaya Media Servers, on page 4-4 and Related Documents, on page 1-5.
IP Addresses	DHCP (strongly recommended)	DHCP and TFTP, on page 4-5, and especially DHCP, on page 4-6.
	TFTP settings file	DHCP and TFTP, on page 4-5 and Administering Options for the 4600 Series IP Telephones, on page 4-28.
	Manual administration at the phone	See "Static Addressing Installation" in Chapter 3 of the *4600 IP Telephone Installation Guide.*
Tagging and VLAN	DHCP	DHCP and TFTP, on page 4-5, and Administering Options for the 4600 Series IP Telephones, on page 4-28.
	TFTP settings file (strongly recommended)	DHCP and TFTP, on page 4-5 and Administering Options for the 4600 Series IP Telephones, on page 4-28.
	Manual administration at the phone	See "Static Addressing Installation" in Chapter 3 of the *4600 IP Telephone Installation Guide*.
Quality of Service	DHCP	DHCP and TFTP, on page 4-5, and Administering Options for the 4600 Series IP Telephones, on page 4-28.
	TFTP settings file (strongly recommended)	DHCP and TFTP, on page 4-5, and Administering Options for the 4600 Series IP Telephones, on page 4-28.
	Manual administration at the phone	See "QOS Option Setting" in Chapter 3 of the *4600 IP Telephone Installation Guide*.

Table 4-1. Administration Alternatives and Options for 4600 Series IP Telephones—*Continued*

Parameter(s)	Administrative Mechanisms	For More Information See:
Interface	DHCP	DHCP and TFTP, on page 4-5, and Administering Options for the 4600 Series IP Telephones, on page 4-28.
	TFTP settings file (strongly recommended)	DHCP and TFTP, on page 4-5, and Administering Options for the 4600 Series IP Telephones, on page 4-28.
	Manual administration at the phone	See "Secondary Ethernet (Hub) Interface Enable/Disable" in Chapter 3 of the *4600 IP Telephone Installation Guide*.
SSON	DHCP	Customizing the Site-Specific Option Number (SSON), on page 4-31; DHCP and TFTP, on page 4-5, and especially DHCP, on page 4-6.
	TFTP settings file (strongly recommended)	Customizing the Site-Specific Option Number (SSON), on page 4-31; DHCP and TFTP, on page 4-5, and especially TFTP, on page 4-17s.
	Manual administration at the phone	See "Site-Specific Option Number Setting" in Chapter 3 of the *4600 IP Telephone Installation Guide*.
Application-specific parameters	DHCP	DHCP and TFTP, on page 4-5, and especially DHCP, on page 4-6. Also, Customizing the 4630/4630SW IP Telephone, on page 4-33 and Customizing the 4620 IP Telephone, on page 4-39.
	TFTP settings file (strongly recommended)	DHCP and TFTP, on page 4-5, especially TFTP, on page 4-17. Also, Customizing the 4630/4630SW IP Telephone, on page 4-33 and Customizing the 4620 IP Telephone, on page 4-39.

General information about administering DHCP servers is covered in DHCP and TFTP, on page 4-5, and more specifically, DHCP, on page 4-6. General information about administering TFTP servers is covered in DHCP and TFTP, on page 4-5, and more specifically, TFTP, on page 4-17.

Once you are familiar with that material, you will be able to administer options on the telephone in accordance with Administering Options for the 4600 Series IP Telephones, on page 4-28.

NOTE If a given parameter is administered in multiple places, the last server to provide the parameter has precedence. The sequence is: manual administration, DHCP, TFTP, and then the call server. That means, for parameters downloaded by the call server, any previous settings, including manual settings, are overwritten by the setting the Avaya IP Telephone receives from the call server. The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, the usual sequence applies through TFTP. If the VLAN ID after TFTP is non-zero, any VLAN ID from the call server is ignored.

Administering 4600 Series IP Telephones on Avaya Media Servers

DEFINITY® Releases 9, 9.5, 10, and Avaya™ Communication Manager Software Release 1.1+

DEFINITY® Releases 9 and 9.5 provide support for the 4606, 4612, and 4624 IP Telephones. DEFINITY® Release 10 adds support for the 4630 and 4630SW IP Telephones. Avaya™ Communication Manager Software Release 1.1 adds support for the 4602/4602SW and 4620 IP Telephones. Administration of a 4612 and 4624 IP telephone is identical to a 6424 IP softphone. See Related Documents, on page 1-5, particularly the *Administration for Network Connectivity* and the *Administrator's Guides*. Follow these guidelines:

- On the Customer Options form, verify that the **IP Stations** field is set to "y." If it is not, contact your Avaya sales representative.
- The **IP Softphone** field does not have to be set to "y."

DEFINITY® Release 8.4

NOTE DEFINITY® Release 8.4 is very old and is not recommended.

DEFINITY® Release 8.4 supports the 4612 and 4624 IP Telephones. The 4612 and 4624 IP Telephones are aliased as 6424 telephones, administered as IP Softphones. The administrative forms for the 6424 IP Softphone are used for the two IP Telephones. See Related Documents, on page 1-5, particularly the *Administration for Network Connectivity* and the *Administrator's Guides*. Follow these guidelines:

- Alias the IP Telephone as a 6424D+ DCP set, with the **IP Softphone** field set to "y."
- Administer a **Media Complex Ext** for the audio channel.

DHCP and TFTP

Dynamic Host Configuration Protocol (DHCP) provides a means by which configuration parameters can be automatically assigned to clients on a TCP/IP network. This minimizes the maintenance of a 4600 Series IP Telephone network by removing the need to individually assign and maintain IP addresses and other parameters for each IP telephone on the network.

Software Checklist

Please make sure that you have purchased and/or own licenses to install and use the DHCP server and TFTP server software.

NOTE It is possible to install both the DHCP server and the TFTP server on the same machine.

WARNING:

*The circuitry in the 4600 Series IP Telephones reserves IP addresses of the form **192.168.2.x** for internal communications. The telephone(s) will not properly use addresses you specify if they are of that form.*

Required Network Information

DHCP is the control point where an enterprise controls its IP Telephones. Before administering DHCP and TFTP, complete the information in Table 4-2, on page 4-6 below to ensure that you have the necessary information regarding your network. There may be more than one Gateway, TFTP server, subnet mask and CLAN in your configuration. You will need a copy of this table for each DHCP server.

Release 1.5 of the 4600 Series Telephones supported the ability to specify a list of IP addresses for a gateway/router, TFTP server, and Avaya media server CLAN board(s), as explained in Overview of Voice over IP (VoIP), on page 2-1. Each list may contain up to 127 total ASCII characters, with IP addresses separated by commas with no intervening spaces.

When specifying IP addresses for the TFTP server or call server, you can use either dotted decimal format (“xxx.xxx.xxx.xxx”) or DNS names to identify the address(es). If you use DNS, note that the system value DOMAIN will be appended to the IP addresses you specify. If DOMAIN is null, the DNS names must be fully qualified, in accordance with IETF RFCs 1034 and 1035. For more specific information about DNS, see DHCP Generic Setup, on page 4-7 and DNS Addressing, on page 4-31.

Table 4-2. Required Network Information Before Installation - Per DHCP Server

1.	Gateway (router) IP address(es)	
2.	TFTP server IP address(es)	
3.	Subnet mask	
4.	DEFINITY®/MultiVantage™ CLAN IP address(es)	
5.	Avaya media server CLAN port	Although this may be a value between 0 and 65535, the default value is 1719 and **should not** be changed unless this conflicts with an existing port assignment.
6.	TFTP server file path	
7.	Telephone IP address range *From:* *To:*	
8.	DNS Server address(es)	If applicable

The **TFTP server file path** is the "root" directory used for all transfers by the server. This is the default directory all files will be uploaded to or downloaded from. In configurations where the upgrade script and application files are in the default directory, see item 6 in Table 4-2, on page 4-6 should not be used.

DHCP

This section provides basic information on DHCP servers and generic information on DHCP server administration.

Choosing a DHCP Configuration

A discussion on how to best set up your network to work with the 4600 Series IP Telephones is beyond the scope of this document. See Network Assessment, on page 2-5. This document concentrates on the simplest case of the single LAN segment. Information provided here can be extrapolated for more complex LAN configurations.

WARNING:

Before you start, it is important that you understand your current network configuration. An improper installation can cause network failures or reduce the reliability and performance of your network.

DHCP Software Alternatives

Two DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server

Any other DHCP application may work.

It is the customer's responsibility to install and configure the DHCP server correctly. This document is limited to describing a generic administration that will work with the 4600 Series IP Telephones.

DHCP Generic Setup

Set up of a DHCP server involves the following phases:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with the following information:
   - IP addresses available for the 4600 Series IP Telephones.
   - Lease duration (Infinite is recommended).
   - The following DHCP options:
     - — Gateway (router) IP address(es) (Table 4-2, on page 4-6, item 1). If more than one address is listed, the total list may contain up to 127 total ASCII characters, with IP addresses separated by commas with no intervening spaces.
     - — Subnet mask (Table 4-2, on page 4-6, item 3).
     - — Option 6 (DNS server(s) address list). If more than one address is listed, the total list may contain up to 127 total ASCII characters, with IP addresses separated by commas with no intervening spaces. At least one address in Option 6 must be a valid, non-zero, dotted decimal address - otherwise, DNS will fail.
     - — Option 15 (DNS Domain Name). This string should contain the domain name to be used when DNS names in system parameters are resolved into IP addresses. This domain name is appended to the DNS name before the 4600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you wish to use a DNS name for the TFTP server; otherwise, you may specify a DOMAIN as part of TFTP customization, as indicated in DNS Addressing, on page 4-31.
     - — Option 66 (TFTP Server Name).

NOTE Microsoft DHCP servers support only dotted-decimal format for TFTP addresses, not symbolic names. Option 66 need not be used if the TFTP server is identified in the Site Specific Option string (Option 176). However, to simplify configuration, we recommend that you use Option 66. If you use both Option 66 and Option 176 to identify TFTP servers, the value(s) in Option 176 will override the value(s) in Option 66.

— A 4600 Series IP Telephone-specific DHCP option specifying information such as TFTP server and DEFINITY®/MultiVantage™ CLAN IP addresses. Use the site-specific option (SSON) at #176. The value for this option should be set to either of the following strings:

MCIPADD=xxx.xxx.xxx.xxx,MCPORT=yyyy,TFTPSRVR=zzz.zzz.zzz.zzz,TFTPDIR=<path>

OR

MCIPADD={list of DNS names},MCPORT=yyyy,TFTPSRVR={list of DNS names},TFTPDIR=<path>

Where xxx.xxx.xxx.xxx is one or more IP addresses for DEFINITY®/MultiVantage™ CLAN IP boards, yyyy is the DEFINITY/MultiVantage CLAN port (1719), zzz.zzz.zzz.zzz is one or more IP addresses for TFTP servers, and <path> is the location of the location of the upgrade script and application files on the TFTP server as entered in Table 4-2, on page 4-6, items: 4, 5, 2, and 7, respectively. Each list may contain up to 127 total ASCII characters, with IP addresses separated by commas with no intervening spaces, and with quotes on either end (see the example in the **NOTES** below). If you use DNS, note that the system value DOMAIN will be appended to the IP addresses you specify. If DOMAIN is null, the DNS names must be fully qualified.

The 4600 Series IP Telephones do not support Regular Expression Matching, and therefore, do not use wildcards. See Administering Options for the 4600 Series IP Telephones, on page 4-28.

In configurations where the upgrade script and application files are in the default directory, the TFTPDIR=<path> should not be used.

You do not have to use Option 176, but if you do not use it, you must ensure the key information (TFTPSRVR, MCIPADD, and MCPORT, especially) is administered appropriately elsewhere. For example, if the DNS server is specified in Option 6, and the Domain Name is specified in Option 15, you can use the configured names "AvayaTFTPServer" and "AvayaCallServer" for TFTPSRVR and MCIPADD, respectively. Upgrading from IP Telephone Releases prior to R1.60 requires Option 176 to be administered with, at a minimum, MCIPADD.

DHCP servers should be administered to deliver only the options specified in this document. Administering additional, unexpected options may have unexpected consequences, including possibly causing the IP Telephone to ignore the DHCP server.

The Call Server Name, TFTP Server Name, and SMTP Server Name must each be no more than 32 characters in length.

NOTES

- Examples of good DNS administration include the following:
  - Option 6: “aaa.aaa.aaa.aaa”
  - Option 15: “dnsexample.yourco.com”
  - Option 66: “tftpserver.yourco.com,zzz.zzz.zzz.zzz”
  - Option 176: “MCIPADD=xxxx.xxx.xxx.xxx”
- Depending on the DHCP application you choose, you should be aware of the fact that the application most likely will not immediately recycle expired DHCP leases. An expired lease may remain reserved for the original client for a day or more (for example, Windows NT® DHCP reserves expired leases for about one day). The intent of this reservation period is to protect a client’s lease in case the client and the DHCP server are in two different time zones, the computers’ clocks are not in synch, or the client is not on the network when the lease expires.
- The implication of this fact may be seen in the following example: Assume 2 IP addresses (hence two possible DHCP leases) and three IP telephones, two of which are using the two available IP addresses. When the lease expires for the first two telephones, the third will not be able to get a lease (even if the other two telephones have been removed from the network) until the reservation period expires.

The 4600 Series IP Telephone sets the indicated system values to the values of the indicated fields of the DHCPACK message as indicated in Table 4-3 below.

Table 4-3. DHCPACK Setting of System Values

System Value	Set to
IPADD	The yiaddr field.
NETMASK	Option #1 (if received).
GIPADD	The first four octets of option #3 (if received).
TFTPSRVR	The first four octets of the siaddr field.

The remainder of this section describes some common DHCP servers.

Windows NT® 4.0 DHCP Server

This section contains details on how to verify and configure the DHCP server included in the Windows NT® 4.0 server operating system.

Use Verifying the Installation of the DHCP Server below to verify whether the DHCP server is installed. If it is not, install the DHCP server. If it is installed, go to the section Initial Configuration, on page 4-10 and the following section.

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**→**Settings**→**Control Panel**.
2. Double-click the **Network** icon.
3. Verify that **Microsoft DHCP Server** is listed as one of the Network Services on the Services tab.
4. If it is listed, go to the section Initial Configuration below. If it is not listed, then install the DHCP server.

Initial Configuration

The Windows NT® 4.0 DHCP server configuration involves setting up a scope for the IP telephone. A DHCP scope is essentially a grouping of IP devices (in this case IP telephones) running the DHCP client service in a subnet. The scope is used to define parameters for each subnet. Each scope has the following properties:

- A unique subnet mask used to determine the subnet related to a given IP address.
- A scope name assigned by the administrator when the scope is created.
- Lease duration values to be assigned to DHCP clients with dynamic addresses.

In addition, the DHCP server can assign configuration parameters to a client, and these can be specified for each individual DHCP scope.

Setting up the Windows NT® 4.0 DHCP server requires the following steps:

1. Creating a DHCP scope for the IP Telephones.
2. Editing custom options.
3. Adding the DHCP options.
4. Activating the new scope.

Each step is detailed in the next four sub-sections.

Creating a DHCP Scope for the IP Telephones

Use the following procedure to create a DHCP scope for the IP Telephones.

1. Select **Start**→**Programs**→**Admin Tools**→**DHCP Manager**.
2. Expand **Local Machine** in the DHCP Servers window by double clicking on it until the **+** sign changes to a **-** sign.
3. Select **Scope**→**Create**.

4. Define the range of IP addresses used by the IP telephones listed in Line 7 of Table 4-2, on page 4-6.

   The **Start Address** should be the first IP address to be used for the IP telephones.

   The **End Address** should be the last IP address to be used for the IP telephones.

   The **Subnet Mask** should be set to the value as recorded in Table 4-2, on page 4-6.

   Perform the next four steps to ***exclude*** any IP addresses that you do not want assigned to IP telephones within the range specified by the Start and End Addresses.

   a. In the **Exclusion Range Start Address** field, enter the *first IP address in the range that you want to exclude*.

   b. In the **Exclusion Range End Address** field, enter the *last IP address in the range that you want to exclude*.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range to be excluded.

      Example:

      Suppose the range of IP addresses available for your IP telephone network are:

      - 135.254.76.7 to 135.254.76.80
      - 135.254.76.90 to 135.254.76.200
      - 135.254.76.225 to 135.254.76.230

      Your start address and end address should then be 135.254.76.7 and 135.254.76.230 respectively.

      You should exclude the ranges 135.254.76.81 to 135.254.76.89 and 135.254.76.201 to 135.254.76.224.

      NOTES
      - We recommend that you provision the 4600 Series IP Telephones with sequential IP addresses.
      - We recommend not mixing 4600 Series IP Telephones and PCs in the same scope.

5. Under **Lease Duration**, select the **Limited To** option and set the *lease duration* to the maximum.
6. Enter a *sensible name* for the **Name** field, such as “DEFINITY IP Telephones.”
7. Click **OK**.

   A dialog box prompts you: **Activate the new scope now**?
8. Click **No**.

   NOTE Activate the scope only after setting all options.

Editing Custom Options

Use the following procedure to edit custom options.

1. Highlight the newly-created scope.
2. Select **DHCP Options→Defaults** in the menu.
3. Click the **New** button.
4. In the **Add Option Type** dialog box, enter an appropriate custom option name, for example, "46XXOPTION".
5. Change the **Data Type Byte** value to **String**.
6. Enter **176** in the **Identifier** field.
7. Click the **OK** button.

   The DHCP Options menu displays.
8. Select the **Option Name** for 176 and set the *value string*.
9. Click the **OK** button.
10. For the **Option Name** field, select **003 Router** from the drop-down list.
11. Click **Edit Array**.
12. Enter the *Gateway IP address* recorded in Line 1 of Table 4-2, on page 4-6 for the **New IP Address** field.
13. Select **Add** and then **OK**.

Adding the DHCP Option

Use the following procedure to add the DHCP option.

1. Highlight the scope you just created.
2. Select **Scope** under DHCP OPTIONS.
3. Select the **176 option** that you created from the Unused Options List.
4. Click the **Add** button.
5. Select **option 003** from the Unused Options List.
6. Click the **Add** button.
7. Click the **OK** button.
8. Select the **Global parameter** under DHCP Options.
9. Select the **176 option** that you created from the Unused Options List.
10. Click the **Add** button.
11. Click the **OK** button.

Activating the Leases

Use the following procedure to activate the leases.

1. Click **Activate** under the Scope Menu.

   The light-bulb icon for the scope lights.

Verifying Your Configuration

This section describes how to verify that the 46XXOPTIONs are correctly configured for the Windows NT® 4.0 DHCP server.

Verify the Default Option, 176 46XXOPTION

Use the following procedure to verify the default option.

1. Select **Start→Programs→Admin Tools→DHCP Manager**.
2. Expand “Local Machine” in the DHCP Servers window by double clicking on it until the + sign changes to a - sign.
3. In the DHCP Servers frame, click the *scope* for the IP Telephone.
4. Select **Defaults** from the **DHCP_Options** menu.
5. In the Option Name pull-down list, select **176 46XXOPTION**.
6. Verify that the Value String box contains the correct string from DHCP Software Alternatives, on page 4-7.

   If not, update the string and click the **OK** button twice.

Verify the Scope Option, 176 46XXOPTION

Use the following procedure to verify the scope option:

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click on **176 46XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup, on page 4-7.

   If not, update the string and click the **OK** button.

Verify the Global Option, 176 46XXOPTION

1. Select **Global** under DHCP OPTIONS.
2. In the **Active Options:** scroll list, click **176 46XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup, on page 4-7. If not, update the string and click the **OK** button.

Windows 2000® DHCP Server

This section describes the configuration of the DHCP server in Windows 2000®.

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**→**Program**→**Administrative Tools**→**Computer Management**.
2. Under **Services and Applications** in the Computer Management tree, you should find **DHCP**.
3. If DHCP is not installed, install the DHCP server; otherwise proceed directly to Creating and Configuring a DHCP Scope, on page 4-14 for instructions on server configuration.

Creating and Configuring a DHCP Scope

Use the following procedure to create and configure a DHCP scope.

1. Select **Start**→**Programs**→**Administrative Tools**→**DHCP**.
2. In the console tree, click the *DHCP server* to which you wish to add the DHCP scope for the IP telephones. Typically this will simply be the name of your DHCP server machine.
3. Select **Action**→**New Scope** from the menu.

   Windows displays the New Scope Wizard to guide you through rest of the setup.
4. Click the **Next** button.

   The Scope Name dialog box displays.
5. In the **Name** field, enter a name for the scope such as "DEFINITY IP Telephones," then enter a brief comment in the **Description** field.
6. When finished, click the **Next** button.

   The IP Address Range dialog box displays.
7. Define the range of IP addresses used by the IP telephones listed in item 7 in Table 4-2, on page 4-6. The **Start IP Address** should be the first IP address available to the IP telephones. The **End IP Address** should be the last IP address available to the IP telephones.

   NOTE We recommend not mixing 4600 Series IP Telephones and PCs in the same scope.

8. Define the *subnet mask* in one of two ways:
   - The number of bits of an IP address to use for the network/subnet IDs.
   - The subnet mask IP address.

   Enter only one of these values and when finished, click the **Next** button.

   The Add Exclusions dialog box displays.

9. Exclude any IP addresses in the range specified in the previous step that you do not wish to be assigned to an IP telephone.

   a. In the **Start Address** field under Exclusion Range, enter the *first IP address in the range you want to exclude*.

   b. In the **End Address** field under Exclusion Range, enter the *last IP address in the range you want to exclude.*

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range that you would like to exclude.

   NOTE You may add additional exclusion ranges later by right clicking on the Address Pool under the newly created scope and select the New Exclusion Range option.

   Example:

   Suppose the ranges of IP addresses available for your IP telephone network are:

   - 135.254.76.7 to 135.254.76.80
   - 135.254.76.90 to 135.254.76.200
   - 135.254.76.225 to 135.254.76.230

   Your Start IP Address and End IP Address entered on the IP Address Range dialog box should then be 135.254.76.7 and 135.254.76.230 respectively.

   On the Add Exclusions dialog box, you should exclude the following ranges:

   - 135.254.76.81 to 135.254.76.89
   - 135.254.76.201 to 135.254.76.224

   Click the **Next** button when all the exclusions have been entered.

   The Lease Duration dialog box displays.

10. For all telephones that will receive their IP addresses from the server, enter **30 days** in the **Lease Duration** field. This is the duration after which a device's IP address expires and needs to be renewed by the device.

11. Click the **Next** button.

    The Configure DHCP Options dialog box displays.

12. Click the **No, I will activate this scope later** radio button.

    The Router (Default Gateway) dialog box displays.

13. For each router or default gateway, enter the IP address and click the **Add** button.

    When you are done, click the **Next** button.

    The Completing the New Scope Wizard dialog box displays.

14. Click the **Finish** button.

    The new scope appears under your server in the DHCP tree. The scope is not yet active and will not assign IP Addresses.

15. Highlight the *newly created scope* and select **Action→Properties** from the menu.
16. Under **Lease duration for DHCP clients**, select **Unlimited** and then click the **OK** button.

WARNING:

IP Address leases are kept active for varying periods of time. To avoid having calls terminated suddenly, make the lease duration unlimited.

Adding DHCP Options

Use the following procedure to add DHCP options to the scope you created in the previous procedure.

1. On the DHCP window, right-click the "Scope Options" folder under the scope you created in the last procedure.

   A drop-down menu displays.

2. Click the **Configure Options...** option.

   The Scope Options dialog box displays.

3. In the General tab page, under the **Available Options**, check the 066'Boot Server Host Name' Options checkbox.

   The String Value dialog box displays.

4. Enter the *TFTP Server address(es)* in the **String Value**. Use the same TFTPSRVR *value* format as discussed in TFTP Generic Setup, on page 4-18. For example, if you had a TFTP server at IP address *zzz.zzz.zzz.zzz* and a second TFTP server at address tftpserver.yourco.com, in the string value enter:

   "zzz.zzz.zzz.zzz,tftpserver.yourco.com"

5. In the left pane of the DHCP, right click on the name of the DHCP Server, then click on **Set Predefined Options...**.
6. Under **Predefined Options and Values**, click on **Add**.
7. In the **Option Type Name** field, enter any appropriate name, for example, "Avaya IP Telephones".
8. Change the **Data Type** to **String**.
9. In the **Code** field, enter **176**, then click the **OK** button twice.

   The Predefined Options and Values dialog box closes, leaving the DHCP dialog box enabled.

10. Expand the newly created scope to reveal its Scope Options.
11. Click **Scope Options** and select **Action→Configure Options** from the menu.
12. In the General tab page, under the **Available Options**, check the **Option 176** checkbox.

13. In the **Data Entry** box, enter the *DHCP IP telephone option string* as described in DHCP Generic Setup, on page 4-7.

    NOTE You can enter the text string directly on the right side of the Data Entry box under the ASCII label.

14. From the list in **Available Options**, check option **003 Router**.
15. Enter the *gateway (router) IP address* as recorded in the IP Address field of Table 4-2, on page 4-6.
16. Click the **Add** button.
17. Click the **OK** button.

Activating the New Scope

Use the following procedure to activate the new scope.

1. In the DHCP console tree, click the *IP Telephone Scope you just created*.
2. From the Action menu, select **Activate**.

   The small red down arrow over the scope icon disappears, indicating that the scope has been activated.

TFTP

This section describes how to set up a TFTP server for downloading software updates to the 4600 Series IP Telephones.

WARNING:

The files defined by the TFTP server configuration have to be accessible from all IP Telephones. Ensure that the filenames match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

NOTE You can use any TFTP application you want. However, we strongly recommend using the TFTP application available for free download at http://www.avaya.com/support.The site also contains instructions for installing and configuring the Avaya TFTP server.

TFTP Generic Setup

The following phases are involved in setting up a TFTP server.

- Install the TFTP server software. The section below describes how to install and configure Avaya's TFTP application.
- Configure the file path parameter to the directory where the files are to be stored. This is the file path in line 6 of Table 4-2, on page 4-6. For increased security, it is also recommended that you disable the ability to upload to the server. Note that this option may be not available to all TFTP servers.
- You may also enable the transfer size option (tsize) if your TFTP server supports it. Doing so allows the IP telephone to monitor the transfer's progress by displaying the total number of data blocks.
- Download the upgrade script file and application file from the Avaya website (http://www.avaya.com/support) to the directory as specified by the file path.

Avaya TFTP (Suite Pro)

Configuration

Use the following procedure to configure the Avaya TFTP server.

1. Run the TFTP Suite Pro server by selecting **Start→Programs→Avaya TFTP Server→TFTPServer32**.

   The TFTP server starts.

   WARNING:

   You must re-start Avaya TFTP manually every time you reboot your TFTP server machine.

2. Select **System→Setup**.
3. Enter the following values:

   On the Outbound tab page: 1.

   The Outbound path is the TFTP file path as recorded in Table 4-2, on page 4-6, Required Network Information Before Installation - Per DHCP Server.

   The **Enable Path** options should be checked.

   Under the Options tab page: turn on the **No Incoming** option.

   Under the Client Limits tab page: Drag the slide bar all the way to the right to set the **Maximum Simultaneous Clients** to infinite.

4. Place the *46xxupgrade.scr* file in the file path directory. (The filename *46xxupgrade.scr* is an example, not the filename you will use. See Contents of the Upgrade Script, on page 4-21.)

4600 Series IP Telephone Scripts and Application Files

The files necessary to operate the 4600 Series IP Telephones are available on the Avaya web site at: http://www.avaya.com/support

Two files on the TFTP Server are essential, other files will be needed when the Avaya IP Telephones need to be upgraded. The essential files are:

NOTE The 4630 telephones have a different upgrade process than the other telephones. This is because the 4630 touch screen operation is significantly more complex than any of the other Avaya IP Telephones. There are some common elements between the 4630 and other IP Telephones; any differences are highlighted as appropriate in this section.

- An upgrade script file, which tells the IP telephone whether it needs to upgrade software. The Avaya IP Telephones attempt to read this file every time they reset. The upgrade script file is also used to point to the settings file. There are separate upgrade script files for the 4630 telephones.
- The settings file contains the option settings that enable many of the options you will need to customize the Avaya IP Telephones for your enterprise. You can use one settings file for all of your Avaya IP Telephones.

In addition to the two upgrade scripts and the settings file you need the latest binary code used in the Avaya IP Telephones.

These files are available from the Avaya website, thereby allowing you to upgrade to new software releases and new functionality without having to replace IP telephones. In general, all these files, plus other useful information such as a ReadMe file, information about infrared capabilities, and a template for the settings file, are contained in a self-extracting executable file (in both zipped and unzipped format) you can download to your TFTP server. Typically, application files for all the 4600 Series IP Telephones are bundled together in that self-extracting executable file - with the exception of the 4630/4630SW, which bundles its boot file and application file, plus the other useful information mentioned, in a separate, self-extracting executable file.

The Avaya-provided upgrade script files, and the binaries included in the zip files, are designed to upgrade the Avaya IP Telephones. You should not normally need to modify them. It is essential that all of the binary files be together on the TFTP server. When downloading a new release onto a TFTP file server with an existing release already on it, we recommend that you:

- Stop the TFTP server.
- Back up all the current TFTP directories.
- Copy your 46xxsettings.txt file to a backup location.
- Remove all of the files in the download directory. This will ensure you do not have an inappropriate binary or configuration file on the server.
- Download the self-extracting executable file (or zip file if you prefer).

- Extract all of the files. When extracting the 4630 files, be sure to allow the directories to be created.
- Copy your 46xxsettings.txt file back into the download directory.
- Check the Readme files for release-specific information.
- Modify the 46xxsettings.txt file as desired.
- Restart the TFTP Server.
- Reset your Avaya IP Telephones.

You can download a default upgrade script file, sometimes called merely the "script file" or the "settings file," from avaya.com/support. This file is sufficient to allow the telephone to use default settings for customer-definable options, although of course these settings can also be changed with DHCP or in some cases, from the telephone's dialpad itself. However, you might want to open the default file and administer the options to add useful functionality to your Avaya IP Telephones. This file must reside in the same directory as the upgrade script file, and must be called **46xxsettings.scr** or **46xxsettings.txt.** The Avaya IP Telephones can operate without this file.

NOTE Most Windows systems interpret the file extension *.scr as a screen saver. The 4600 IP Telephones originally used *.scr to indicate a script file, but starting with Release 1.7, the settings file can also have the extension *.txt.

The settings file must consist of SET commands, one per line, in this format:

SET *parameter_name* value

where *parameter_name* and value are as defined in Table 4-5, on page 4-29 (parameters, descriptions, and acceptable values for all 4600 Series IP Telephones), Table 4-6, on page 4-34 (parameters, descriptions, and acceptable values specific to 4630/4630SW IP Telephone applications), and Table 4-7, on page 4-39 (parameters, descriptions and acceptable values specific to 4620 IP Telephone applications). Invalid values cause the specified value to be ignored for the associated *parameter_name* (so the default value is retained). All values should be text strings, even if the value itself is numeric, a dotted decimal IP address, etc.

NOTE All data should be enclosed in quotation marks for proper interpretation.

The Avaya-provided upgrade script file includes lines that tell the telephone to GET **46xxsettings.scr** and **46xxsettings.txt.** These lines cause the telephone to use TFTP to attempt to download the file specified in the GET command. If the file is successfully obtained, its contents are interpreted as an additional script file - that is how your settings are changed from the default settings. If the file cannot be obtained, the telephone continues processing the upgrade script file (so if you do not have a **46xxsettings.scr** file, the telephone will look for a **46xxsettings.txt** file). If the settings file is successfully obtained but does not include any setting changes (which is the case when you initially download the script file template from the Avaya Support website, before you make any changes), the telephone stops using TFTP (and hence, does not go back to the upgrade script file).

You can change the name of the settings file, if desired, as long as you also edit the corresponding GET command in the upgrade script file. In general, however, you are encouraged not to alter the Avaya-provided upgrade script file; if Avaya changes the upgrade script file in the future, any changes you have made will be lost. You are strongly encouraged to use the **46xxsettings** file to manage your customization instead.

Contents of the Upgrade Script

The following is a sample upgrade script file:

NOTE The filenames following the SET APPNAME command in this sample are examples only and may not match those used in production.

```
####################################
#Copyright Avaya 2003              #
#All rights reserved               #
####################################
#check bootApp version      #
####################################
IF $MODEL4 SEQ 4602 goto BOOTAPP4602
IF $MODEL4 SEQ 4606 goto BOOTAPP46XX
IF $MODEL4 SEQ 4612 goto BOOTAPP46XX
IF $MODEL4 SEQ 4620 goto BOOTAPP4620
IF $MODEL4 SEQ 4624 goto BOOTAPP46XX
goto END
# BOOTAPP4602
IF $BOOTNAME SEQ bb4602r1_61.bin goto DEF46XX
SET APPNAME bb4602r1_61.bin
goto END
# BOOTAPP4620
IF $BOOTNAME SEQ 4620COMMON.V1719 goto DEF46XX
SET APPNAME bbla20_1719.bin
goto END
# BOOTAPP46XX
IF $BOOTNAME SEQ 46XXCOMMON.V36 goto DEF46XX
IF $BOOTNAME SEQ 46XXCOMMON.V52 goto DEF46XX
IF $BOOTNAME SEQ 46XXCOMMON.V69 goto DEF46XX
SET APPNAME bbla0_69.bin
goto END
################################
#download definity bigApp      #
################################
```

```
# DEF46xx
IF $MODEL4 SEQ 4602 goto DEF4602
IF $MODEL4 SEQ 4606 goto DEF4606
IF $MODEL4 SEQ 4612 goto DEF4624
IF $MODEL4 SEQ 4620 goto DEF4620

IF $MODEL4 SEQ 4624 goto DEF4624
goto END

#definity bigApp for 4602 model
# DEF4602
SET APPNAME ap4602r1_61.bin
goto END

#definity bigApp for 4606 model
# DEF4606
SET APPNAME def06r1_73.bin
goto END

#definity bigApp for 4620 model
# DEF4620
SET APPNAME def20r1_73.bin
goto END

#definity bigApp for 4612 & 4624 model
# DEF4624
SET APPNAME def24r1_73.bin
goto END

# END

#####################################

#download the 46xx Settings script #

#####################################

GET 46xxsettings.scr
GET 46xxsettings.txt
```

Contents of the TFTP Settings File

As seen by the last lines of the Upgrade Script file (above), after checking the application software, the 4600 Series IP Telephone looks for a 46xxsettings file. This optional file is under your control and is where you would identify non-default option settings, application-specific parameters, etc. A template for this file is available for download at the Avaya support website, and an example of what the file could look like is displayed below. At the Avaya support website, you can also download a "4600 Settings Wizard," a simple software program that asks a few questions to step you through the automatic creation of a 46xxsettings file.

NOTE The sample below is intended as an example only; your settings will most likely vary from the settings shown. This sample assumes specification of a DNS Server, parameters for the 4630/4630SW Directory application, and a 4620 web browser. See Administering Options for the 4600 Series IP Telephones, on page 4-28, for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

```
DNSSRVR="dnsexample.yourco.com"

DIRSRVR="123,123,123,123"
DIRTOPDN="yourco"

WMLHOME="http://support.avaya.com/elmodocs2/avayaip/4620/home.wml"
WEBPROXY="11.11.11.11"
```

QoS

The 4600 Series IP Telephones support both IEEE 802.1D/Q and DiffServ, and in the future may support other, possibly proprietary, procedures for implementing Quality of Service. In addition, other network-based QoS initiatives such as UDP port selection do not require support by the telephones, but nonetheless can contribute to improved QoS for the entire network.

IEEE 802.1D and 802.1Q

IEEE's 802.1Q standard defines a tag that can be added to voice and data packets. Most of the information associated with this tag deals with Virtual LAN (VLAN) management, but 3 bits are reserved for identifying packet priority. These 3 bits allow any one of 8 priorities to be assigned to a specific packet. As defined in the standard, the 8 priorities are, from highest to lowest:

- 7: Network management traffic
- 6: Voice traffic with less than 10ms latency
- 5: Voice traffic with less than 100ms latency
- 4: "Controlled-load" traffic (mission-critical data applications)
- 3: Traffic meriting "extra-effort" by the network for prompt delivery (for example, executives' e-mail)
- 2: Reserved for future use
- 0: Traffic meriting the network's "best-effort" for prompt delivery (the default priority)
- 1: Background traffic such as bulk data transfers and backups

NOTE Priority 0 is a higher priority than Priority 1.

To support IEEE 802.1D/Q, the 4600 Series IP Telephones can be administered either from the network via appropriate administration of the DHCP or TFTP servers, or at the telephone itself via dialpad input. Specific implementation details for local administration are in the *Installation Manual*, and for remote administration are in this chapter, in 4600 Series IP Telephone Scripts and Application Files, on page 4-19. In summary, three IEEE 802.1D/Q QoS parameters in the telephones can be administered. These parameters are:

- L2Q: setting the 802.1Q framing parameter; 1 (ON), 2 (OFF), or 0 (AUTO); default is 0. Manually setting a specific 4600 IP Telephone's L2Q value to other than AUTO (i.e., either ON or OFF) by means of the QoS Local Administrative Option specified in the *4600 Series IP Telephone Installation Guide* means that the telephone will use the value entered manually, rather than any value you administer via the DHCP or TFTP settings file.
- L2QAUD: setting the 802.1Q audio priority value (between 0 and 7, default is 6)
- L2QSIG: setting the 802.1Q signaling priority value (between 0 and 7, default is 6)

The 4600 Series IP Telephones can simultaneously support receipt of packets using, or not using, 802.1Q parameters.

WARNING:

If you turn VLAN framing on (L2Q=1) using the TFTP-based upgrade script (46xxupgrade.scr), and you set your VLAN ID (L2QVLAN) to something other than your default VLAN ID, the IP address you are using for the telephone will probably be wrong for the new VLAN. See VLAN Considerations, on page 4-27, for more information.

DIFFSERV

As defined in IETF RFCs 2474 and 2475, "services" are basically ways of treating different subsets of a network's traffic in different ways at the Internet Protocol (IP) layer, Layer 3. For example, some packets might be routed in such a way as to expedite delivery (minimize delay), while others are routed to minimize loss, minimize cost, etc. The differentiation between these services (that is, Differentiated Services) is provided by a redefinition of an octet in the Layer 3 headers for IP versions 4 and 6, also termed IPv4 and IPv6, respectively. This octet is called a Type of Service (TOS) octet in IPv4 and a Traffic Class octet in IPv6, but in both cases the octet is interpreted differently than it was originally defined. With Differentiated Services, bits 0 through 5 of the octet identify a Differentiated Services Code Point (DSCP) that identifies a procedure to be used to handle that packet on a per-hop basis. Bits 6 and 7 of the octet are currently unused, and are ignored by DSCP-compliant routers.

With DiffServ, the default DSCP is all zeroes, and represents "no special handling." RFC 2474 also defines eight "Class Selector Codepoints," which are the eight DSCP encodings that can be represented by xxx000 (where "x" represents one bit). These Code Selector Codepoints are considered prioritized, with the larger numerical values having a higher relative order. DSCP-compliant routers should treat larger-valued DSCPs in such a way as to give the associated packets a "probability of timely forwarding" greater than a packet with a lower-valued DSCP. In addition to the eight Class Selector Codepoints, a network may define its own DSCPs by defining encodings that do not terminate in 000. The specific treatment intended by these custom DSCPs will not necessarily be carried out by routers outside the customer's own network.

The Avaya IP Telephones' DiffServ values will be changed to the values administered on the call server as soon as the phone is registered. For more information, see the document titled *Administration for Network Connectivity* (555-233-504). Unless there is a specific need in your enterprise LAN, we do not recommend you change the default values.

UDP Port Selection

Some data networks include equipment that can perform UDP port selection. This is a mechanism by which packets with port numbers in a given range are given priority over packets with port numbers outside that range.

To support UDP port selection, the 4600 Series IP Telephones can be administered either from the network via appropriate administration of the DHCP or TFTP servers, or at the telephone itself via dialpad input. Specific implementation details for local administration are in the *4600 Series IP Telephone Installation Guide*, and, for remote administration, in 4600 Series IP Telephone Scripts and Application Files, on page 4-19. In summary, the system value MCPORT represents the port on the TN2302AP board. This port number can be used to administer routers, etc. that support UDP port selection, to maximize the priority given to the voice packets being exchanged between the PBX and the telephone.

The default value for MCPORT is 1719. The switch must be administered to use a port within the proper range for the specific LAN, and the IP Telephone(s) will copy that port. A related parameter is PORTAUD, which is the RTP port used by the switch. In accordance with standards RFC 1889 and 1890, the IP Telephone uses a default value for PORTAUD of 5004. MCPORT and PORTAUD are both administrable (see Administering Options for the 4600 Series IP Telephones, on page 4-28).

Network Audio Quality Display on 4600 Series IP Telephones

As of Release 1.7 for the 4620 and 4630/4630SW telephones, and as of Release 1.8 for the other 4600 Series IP Telephones, the telephone is by default administered to offer the end user an opportunity to monitor network audio performance while on a call. The user guides for each phone go into specific detail on how the user gets to the appropriate screen; this document tells you what the end user can see, and what it means.

For 4620 and 4630/4630SW IP Telephones, the following parameters are displayed in real-time to users on the appropriate screens, while on a call:

Table 4-4. Parameters in Real-Time

Parameter	Possible Values
Audio Connection Present?	*Yes* (if a receive RTP stream has been established) *No* (if a receive RTP stream has **not** been established)
Received Audio Coding	G.711 or G.729
Silence Suppression	*Yes* (if the telephone knows the far-end has silence suppression Enabled) *No* (if the telephone knows the far-end has silence suppression Disabled, or the telephone does not know either way)
Packet Loss	"No data" or a decimal percentage. Late and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	"No data" or an integer number of milliseconds. The number reflects the amount of delay in received audio packets, and includes any look-ahead delay associated with the codec.
One-way Network Delay	"No data" or an integer number of milliseconds. The number is one-half the value RTCP computes for the round-trip delay.
Network Jitter Compensation Delay	"No data" or an integer number of milliseconds reporting the average delay introduced by the telephone's jitter buffer.

For the 4606, 4612, and 4624 IP Telephones, the Network Audio Quality Screen presents the user with a qualitative assessment of the overall audio quality currently being experienced. This assessment is based on separate evaluations of the Packet Loss and the total Network Delay (the sum of Packetization Delay, One-way Network Delay, and Network Jitter Compensation Delay), and consideration of the codec in use. You can disable the display of the Network Audio Quality data and assessment for all sets by setting the system value NTWKAUDIO to a value of "0" as explained in Administering Options for the 4600 Series IP Telephones, on page 4-28.

The implication of this information for LAN administration depends, of course, on the values reported by the user and the specific nature of your LAN (topology, loading, QoS administration, etc.). The major use for this information is to give the user an idea of how network conditions are affecting the audio quality of the current call. It is assumed you have more detailed tools available for troubleshooting the LAN.

RSVP and RTCP

Avaya IP Telephones implement the Resource ReSerVation Protocol (RSVP) to support WAN bandwidth management. RSVP is administered from the call server. Avaya IP Telephones implement the RTP Control Protocol (RTCP) so that Avaya's Voice over IP (VoIP) Monitoring Manager (VMON) software can provide real-time monitoring and historical data of the audio quality of VoIP calls.

Resource ReSerVation Protocol (RSVP) is an IETF-standard protocol used by hosts to request resource reservations throughout a network. RSVP-compliant hosts send messages through a network to receivers, which respond with messages requesting a type of service and an amount of resources (e.g., bandwidth) to carry out that service. The host is responsible for *admitting* (approving) or *rejecting* (denying) the request. In a QoS context, RSVP is used to try to reserve bandwidth in the network for voice calls, on a call-by-call basis. If insufficient bandwidth is available for the target voice quality, a request to use network bandwidth for a voice call will be rejected.

RTP Control Protocol (RTCP), as its name implies, is a protocol that provides control functions for Real-time Transport Protocol (RTP). RTP provides end-to-end network services for real-time data (such as Voice over IP), but does not provide a reservation function, nor does it guarantee any level of QoS. RTCP supplements RTP by monitoring the quality of the RTP services and can provide real-time information to users of an RTP service. In a QoS context, RTCP is valuable for identifying information such as packet loss, 1-way delay (how long a packet has to go from source A to destination B), jitter, etc. RTCP itself does not improve QoS, but it provides information to help identify where problem areas might be.

You cannot change the telephone's RSVP or RTCP parameters directly on the telephone or via TFTP or DHCP administration. The only way to change these parameters is by appropriate administration of the switch. See your DEFINITY®/MultiVantage™ administration material for more detail.

VLAN Considerations

If your LAN environment does not include Virtual LANs (VLANs), ignore this section. Otherwise, this section contains information on how to administer 4600 Series IP Telephones to minimize registration time and maximize performance in a VLAN environment.

The system value L2QVLAN (initially set to "0"), identifies the 802.1Q VLAN IDentifier. This default value indicates "priority tagging" as defined in IEEE 802.IQ Section 9.3.2.3, which specifies that the Ethernet switch in your network closet should automatically insert the default VLAN for the switch port without changing the user priority of the frame (cf. IEEE 802.1D and 802.1Q).

However, you might not want the default VLAN to be used for voice traffic; for example, you may have administered a VLAN specifically for IP telephony. In this case, you need to ensure the switch is configured to allow frames tagged by the 4600 Series IP Telephone through without overwriting or removing them. In addition, you will want to set the system value L2QVLAN to the VLAN ID appropriate for your voice LAN.

Another system value you can administer as of Release 1.8 software, is NVVLANTEST, which stands for the number of seconds the 4600 IP Series Telephone waits for a DHCPOFFER message when using a non-zero VLAN ID (the default is "60" seconds). Using this value insures the telephone can return to the default VLAN if an invalid VLAN ID is administered or if the phone is moved to a port where the value in L2QVLAN is invalid. The default value is fairly long, to allow for the scenario that a major power interruption is causing the 4600 Series IP Telephones to restart, but time should be allowed for network routers, the DHCP/TFTP Servers, etc. to be returned to service. If the telephone is restarted for whatever reason and the NVVLANTEST time limit expires, the telephone assumes the administered VLAN ID is invalid and re-initiates registration with the default VLAN ID.

NOTES

- If the telephone has returned to the default VLAN but must be put back on the L2QVLAN VLAN ID, you need to Reset the telephone according to the procedure in Chapter 3 of the *4600 Series IP Telephone Installation Guide*.
- The telephone will ignore any VLAN ID administered on the call server if a non-zero VLAN ID is administered manually, via DCHP, and/or via TFTP.

Administering Options for the 4600 Series IP Telephones

As indicated in the Introduction, on page 4-1 of this chapter, there are many parameters that can be administered for the 4600 Series IP Telephones. This section explains how to change parameters via the DHCP or TFTP servers. In all cases, you will be setting a system parameter in the telephone to a desired value. Table 4-5 lists the parameter names, their default values, the valid ranges for those values, and a description of each one. For DHCP, the parameters below are set to desired values in the DHCP Option, as discussed in DHCP Generic Setup, on page 4-7 earlier in this chapter. For TFTP, the parameters below are set to desired values in the TFTP Script File, as discussed in Contents of the Upgrade Script, on page 4-21 also earlier in this chapter.

TFTP Scripts are the recommended way to administer options on the 4600 Series IP Telephones. Some DHCP applications have limits on the amount of user-specified information; such limits could be exceeded by the administration required, for example, a 4630 with all applications administered.

You may choose to completely disable the capability to enter or change option settings from the dialpad, as of Release 1.8. As of that Release, a new system value, PROCPSWD, can be set as part of standard DHCP/TFTP administration. If PROCPSWD is non-null and consists of 1 to 7 digits, no local procedures ("dialpad options") can be invoked unless the user enters the value of PROCPSWD after pressing **Mute** or **Hold** (see "Chapter 3" of the *4600 Series IP Telephone Installation Guide)* and before entering the local procedure code.

NOTES

- Because this password is likely stored on the server “in the clear” and is certainly sent to the telephone in the clear, you should not consider PROCPSWD as a high-security technique to inhibit a sophisticated end-user from obtaining access to the local procedures.
- Administering this password disables all local procedures, including V I E W, which is read-only and would not change any settings in any case.

Table 4-5. 4600 Series IP Telephone Customizable System Parameters

Parameter Name	Default Value	Status	Description and Value Range
AGCHAND	1		Automatic Gain Control status for handset (0=disabled, 1=enabled).
AGCHEAD	1		Automatic Gain Control status for headset (0=disabled, 1=enabled).
CTISTAT	1		Computer-Telephony Integration (CTI) Status (1=enabled, 0=disabled).
CTIUDPPORT	49721		CTI UDP listener port (49714 through 49721, inclusive).
DNSSRVR	" " (Null)		Text string containing the IP address of one or more DNS servers (at least one of which must be a valid, non-zero, dotted decimal address.
DOMAIN	“ “ (Null)		Text string containing the domain name to be used when DNS names in system values are resolved into IP addresses.
IRSTAT	1		Text string containing status of Infrared interface (0= off/disabled, 1= on/enabled).
L2Q	0		802.1Q framing (0=auto. 1= on, 2= off).
L2QAUD	6		Layer 2 audio priority value (0 to 7).
L2QSIG	6		Layer 2 audio priority value (0 to 7).
L2QVLAN	0		802.1Q VLAN IDentifier (0 to 4094).
MCPORT	1719		Call server transport-layer port number (0-65535).
NTWKAUDIO	0		Network Audio Quality Assessment Display (1=on, 0=off).
NVVLANTEST	60		Number of seconds to wait for a DCHPOFFER when using a non-zero VLAN ID (1-3 ASCII digits, from “0” to “999”).

Table 4-5. 4600 Series IP Telephone Customizable System Parameters —*Continued*

Parameter Name	Default Value	Status	Description and Value Range
PHNCC	1	Optional	Telephone country code. The administered international country code for the location of the serving MultiVantage™ server. Range: 1-3 digits, from "1" to "999".
PHNDPLENGTH	5	Optional	Telephone dial plan length - the length of the administered dial plan for the serving MultiVantage™ server. Range: 1 or 2 digits, from "3" to "10".
PHNIC	011	Optional	Telephone international access code - the digits dialed to access public network international trunks from the serving Multi-Vantage™ server. Range: 1-4 digits.
PHNLD	1	Optional	Telephone long distance access code - the digit dialed to access public network long distance trunks from the serving MultiVantage™ server. Range: 1 digit or "" (Null).
PHNLDLENGTH	10	Optional	Length of national telephone number - the number of digits in the longest possible national telephone number for the location of the serving MultiVantage™ server. Range: 1 or 2 digits, from "5" to "15".
PHNOL	9	Optional	Outside line access code - the character(s) dialed to access public network local trunks from the serving MultiVantage™ server. Range: 0-2 dialable characters, including "" (Null).
PHY2STAT	1		Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex).
PROCPSWD	" " (Null)		Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits).
RTCPMON	" " (Null)		Text string containing the 4-octet IP Address of the RTCP monitor currently in use.

NOTE Table 4-5 applies to all 4600 Series IP Telephones. The 4630/4630SW and 4620 IP Telephones have additional, optional administration. See Customizing the 4630/4630SW IP Telephone, on page 4-33 and Customizing the 4620 IP Telephone, on page 4-39, below, for more information.

DNS Addressing

As of Release 1.5, the 4600 IP Telephones support DNS addresses as well as dotted decimal addresses. The telephone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6, as indicated in DHCP Generic Setup, on page 4-7. At least one address in Option 6 must be a valid non-zero dotted decimal address - otherwise, DNS will fail. The text string in the system parameter **DOMAIN** (Option 15, see Table 4-5) is appended to the address(es) in Option 6 before the telephone attempts to resolve the DNS address. If Option 6 contains a list of DNS addresses, they are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS via DHCP, you may specify the DNS server and/or Domain name in the TFTP script file (in which case, you should SET the values for DNSSRVR and DOMAIN first; then you may use those names later in the script).

NOTE If Options 6 and 15 are appropriately administered with DNS servers and Domain names respectively, MCIPADD and TFTPSRVR settings need not be specified in the Site Specific Option string.

Customizing the Site-Specific Option Number (SSON)

As discussed in DHCP Generic Setup, on page 4-7, the SSON, defined to be 176 for the 4600 Series IP Telephones, can be set to a string. For each system parameter listed in Table 4-5 that you want to include, append the following to the SSON string:

a comma followed by **`name=value`**

where **`name`** is a parameter name and **`value`** is its associated value. Invalid values will cause the data to be ignored for that **`name`**. Customizing the SSON will affect all telephones associated with that DHCP server.

Entering Options via the Telephone Dialpad

Chapter 3 of the *4600 Series IP Telephone Installation Guide* details how to use the local administrative options.

To customize any or all of the QoS parameters locally, follow the "QoS Option Setting" procedure in Chapter 3 of the *4600 Series IP Telephone Installation Guide*.

To enable or disable the secondary Ethernet hub locally, follow the "Secondary Ethernet (Hub) Interface Enable/Disable" procedure in Chapter 3 of the *4600 Series IP Telephone Installation Guide*.

To view the 4600 IP Telephone system parameters, refer to The View Administration Option, on page 5-10.

Enhanced Local Dialing

The 4620/4630/4630SW IP Telephones have a variety of telephony-related applications (e.g., Speed Dial, Call Log, Web Browser, etc.) which may obtain a telephone number during operation. For example, an incoming Call Log call will obtain the Calling Party Number, while the web browser may obtain a dialable link from a corporate website. Before Release 1.8 software, when the user indicated a desire to call one of these incoming numbers, the 4620/4630/4630SW would first require the user to edit the number, generally by prepending digits to account for dial access codes, country codes if applicable, etc.

As of Release 1.8, the 4620/4630/4630SW can evaluate a raw telephone number and, based on administered parameters, automatically prepend the correct digits, saving the user time and effort. This is the "Enhanced Dialing" feature. The key to this feature's success is the accurate administration of several important values. Table 4-7 summarizes these values and their meanings; that information is expanded upon here.

NOTES

- In all cases, the values to be administered are the values relevant to the location of the Avaya media server to which the 4620/4630/4630SW IP Telephones are registered. Hence, if the telephone was in Japan, but the call server was in the United States, the value of PHNCC would be properly set to "1".
- In all cases, the digits inserted and dialed by the 4620/4630/4630SW are subject to standard Avaya media server features and administration such as Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), etc.

The system values relevant to the Enhanced Dialing Feature are:

- PHNCC; the international country code for the call server (e.g., "1" for the United States, "44" for the United Kingdom, etc.).
- PHNDPLENGTH; the length of the dial plan on the call server.
- PHNIC; the digits dialed from the call server to access public network international trunks (e.g., "011" for the United States).
- PHNLD; the digit dialed to access public network long distance trunks on the call server.

- PHNLDLENGTH; the maximum length, in digits, of the national telephone number for the country in which the MultiVantage™ call server is located.
- PHNOL; the character(s) dialed to access public network local trunks on the call server.

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML website lists a 4-digit phone number as a link on the Human Resources page. A 4620 user selects that link, the 4620 deduces the phone number is part of the corporate network (because the phone number's length is the same as the corporate dialing plan), and dials the number without further processing.

Example: A user notes the web site displayed contains an international phone number that needs to be called and presses "Call." The 4630/4630SW determines the number to be called is from another country code, and prepends the rest of the phone number with PHNOL (to get an outside line) + PHNIC (to get an international trunk). The 4630/4630SW then dials normally, with the Avaya media server routing the call appropriately.

NOTE The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format according to how you administer the parameters indicated in Table 4-7. The algorithm also assumes that international telephone numbers are identified as such in, for example, WML websites, by preceding them with a plus (+) sign, and with a space or some non-digit character following the country code.

Customizing the 4630/4630SW IP Telephone

The 4630/4630SW IP Telephone has some unique and powerful capabilities that take advantage of its large display and access to LAN facilities. If your organization has an LDAP-compliant directory on your LAN, or if your organization has a corporate website suitable for displaying on the 4630's/4630SW's 1/4-VGA display, you will need to provide the telephone with key information about the servers that provide those facilities. Specifically, to administer the 4630/4630SW telephone for the LDAP Directory application or to administer the 4630/4630SW telephone for the Web Access application, you must provide the information called for in Table 4-6, below. This information must be provided in a customized script file, in accordance with 4600 Series IP Telephone Scripts and Application Files, on page 4-19.

CAUTION:

*For the 4630/4630SW to work properly, you must have a 46xxsettings.scr or 46xxsettings.txt file in the same directory as the 4630/4630SW application file. If you do not edit the 46xxsettings.scr file, the 4630/4630SW will use default settings only. The 46xxsettings file is no longer part of the *zip file on the Avaya software download website, but is available as a standalone download. If you already have such a file because you downloaded it for a previous release of the 4630, installing the standalone file will overwrite the original file.*

NOTE The same 46xxsettings.scr file is used by the 4620 and the 4630/4630SW IP Telephones.

In Table 4-6, parameters shown with a *Mandatory* status must be accurate and non-null for the application to work (however, the Avaya Help website will always be available). Parameters with an *Optional* status may be changed to suit your environment; if they are not changed, the defaults will be used.

Table 4-6. 4630/4630SW IP Telephone Customizable System Parameters by Application

Parameter Name	Default Value	Status	Description and Value Range
Phone Application Parameters:			
PHNEMERGNUM	" " (Null)	Optional	Text string of a phone number to be dialed in case of an emergency (e.g., 911)
Directory Application Parameters:			
DIRSRVR	" " (Null)	Mandatory	Text string of dotted decimal IP address, or DNS name, of the server containing the LDAP directory.
DIRTOPDN	" " (Null)	Mandatory	"Directory Topmost Distinguished Name"; text string of the root entry of the LDAP directory. Note that spaces and other special characters may need to be treated as specified in RFC 2253, *Lightweight Directory Access Protocol (v3); UTF-8 String Representation of Distinguished Names.*
DIRFULLNAME	cn	Optional	Text string for the customer-specific label for the database field.
DIRTELNUM	telephoneNumber	Optional	Text string for the customer-specific label for the database field containing telephone numbers. The default is the standard LDAP value.
DIRSRCHTIME	0	Optional	Text string for an integer number of seconds; the maximum duration the LDAP directory should spend searching before reporting completion or failure of the search. The default is LDAP-standard for "unlimited duration."
DIRCODING	Latin 1	Optional	Text string identifying the character set used by the LDAP directory. Besides the default value, "ASCII" is the other valid value.
DIRLDAPPORT	389	Optional	Directory LDAP Port; the port used to exchange LDAP messages with the server.

Table 4-6. 4630/4630SW IP Telephone Customizable System Parameters by Application— *Continued*

Parameter Name	Default Value	Status	Description and Value Range
Stock Ticker Application Parameters:			
STKSTAT	1	Optional	Text string identifying whether the phones are allowed to have the Stock Ticker Application. "1" is the default; "0" disables the Stock Ticker Application.
Voice Mail Application Parameters:			
VMLCODING	ASCII	Optional	Text string identifying the character set used by the Voice Mail Server Application. Besides the default value, other supported values include "Latin 1" and "Unicode". Note that "Unicode" includes support only for the Latin characters of Unicode.
VMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Voice Mail Application.
Web Access Application Parameters:			
WEBHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application.
WEBPROXY	" " (Null)	Optional	Text string containing the IP address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the web pages to be accessed by the user are all on your organization’s intranet.
WEBEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains, separated by commas, up to a total of 127 ASCII characters. This parameter is optional if the web pages to be accessed by the user are all on your organization’s intranet. If WEBPROXY is null, the value of this parameter is ignored.

Table 4-6. 4630/4630SW IP Telephone Customizable System Parameters by Application— *Continued*

Parameter Name	Default Value	Status	Description and Value Range
WEBPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if the web pages to be accessed by the user are all on your organization's intranet. If WEBPROXY is null, the value of this parameter is ignored.
WEBCODING	ASCII	Optional	Text string containing the coding to be used for characters entered in forms on web pages. Besides the default, other supported values include "Latin 1" and "Unicode". Note that "Unicode" includes support only for the Latin characters of Unicode.
Backup/Restore Parameters:			
FTPSRVR	" " (Null)	Mandatory (but can be user-specified)	Text string containing the 4-octet IP Address, for the FTP server to be used for storage and retrieval of 4630/4630SW user information (see 4630/4630SW Backup/Restore, on page 4-36).
FTPDIR	" " (Null)	Optional (and can be user-specified)	Path name for the directory on FTPSRVR used for storage and retrieval of 4630/4630SW user information.

NOTE For assistance in developing local websites tailored to the 4630 IP Telephone's display, see Appendix B, Creating Websites for the 4630/4630SW IP Telephone.

4630/4630SW Backup/Restore

Backup/Restore automatically saves a phone's speed dial button labels and options/parameter settings. When the Automatic Backup option on a 4630/4630SW IP Telephone is set to "Yes" and the FTPSRVR is specified, the FTPSTOR command attempts to save all Speed Dial contents and all system options and (non-password) parameters to the FTP server (specified by FTPSRVR in the directory path specified by FTPDIR). Data is saved in an ASCII text file called "4630data.txt". The System Administrator may optionally specify FTPSRVR and/or FPTDIR via network

administration, however, these values may also be specified by the phone's user, as covered in Chapter 8 of the *4630 IP Telephone User's Guide*. Automatic backup occurs whenever the user executes a Save command on a Speed Dial or Options/Parameter screen.

NOTE If your network includes both 4620 and 4630/4630SW IP Telephones, you need to specify **FTPSRVR** and **FTPDIR** once, and both telephones will use the same server and directory. The different phones will, of course, store data in different files. In addition, users have the ability to specify alternative servers and directories (e.g., their own PCs) for backup and retrievals. Note, though, that unless different users of the same telephone type (e.g., 4620) locally change the FTP Server or Directory, they will all be saving to the same backup file, overwriting each other's saved data.

In addition to Speed Dial labels and associated phone numbers, the following options and non-password parameters are saved during a backup:

Setting/Parameter Name	Type
Idle Timeout	Option
Keyboard Layout	Option
Click Feedback	Option
Edit Dialing	Option
Personalized Ring	Option
Redial	Option
Go to Phone on Incoming Calls	Option
Go to Phone on Originate	Option
Call Timer	Option
Alphabetize Entries?	Option
Call Log Active?	Option
Call Log Automatic Archive	Option
Directory User ID	Parameter
Automatic Backup	Option
FTP Server IP Address	Parameter
FTP Directory Path	Parameter
FTP User ID	Parameter

Setting/Parameter Name	Type
Stock Ticker Active?	Option
STK.*mm*	Parameter
Stock Index DJIA	Option
Stock Index S&P 500	Option
Stock Index Nasdaq	Option
Stock Change	Option
Stock Volume	Option

If the Automatic Backup option is set to "No," speed dial data, options and parameter settings are not saved unless the user forces a one-time backup via the appropriate option (as covered in Chapter 8 of the *4630 IP Telephone User's Guide)*. Restoring backed-up data is done via a separate user option, also covered in Chapter 8 of the *4630 IP Telephone User's Guide.*

NOTE For specific error messages relating to Backup/Restore, see Table , on page 5-14.

Call Log Archive

Automatic archiving of the Call Log occurs when:

- The Call Log Automatic Archive option setting is "Yes" and
- The Call Log is more than 50% filled with unarchived entries, or a new (unarchived) log entry occurs within two hours of the last archive (whichever occurs first).

Call Log Archive automatically saves applicable Call Log entries. When the Call Log Automatic Archive option on a 4630/4630SW IP Telephone is set to "Yes" and the FTPSRVR is specified, the FTP APPE command attempts to save all call log contents to the FTP server (specified by FTPSRVR in the directory path specified by FTPDIR). Data is saved in a file called "4630calllog.txt". The System Administrator may optionally specify FTPSRVR and/or FPTDIR via network administration, however, these values may also be specified by the phone's user as covered in Chapter 8 of the *4630/4630SW IP Telephone User's Guide*. Automatic backup occurs whenever the user executes a Save command on a Speed Dial or Options/Parameter screen.

NOTE For specific error messages relating to Archiving, see Table , on page 5-14.

Customizing the 4620 IP Telephone

The 4620 IP Telephone has some unique and powerful capabilities that take advantage of its display and access to LAN facilities. For example, if your organization has an LDAP-compliant directory on your LAN or a WML website, you need to provide the telephone with key information about the servers providing those facilities. Specifically, you need to provide the information called for in relevant sections of Table 4-7. This information must be provided in a customized script file, in accordance with 4600 Series IP Telephone Scripts and Application Files, on page 4-19.

CAUTION:

*For the 4620 to work properly, you must have a 46xxsettings.scr file in the same directory as the 4620 application file. If you do not edit the 46xxsettings.scr file, the 4620 will use default settings only. The 46xxsettings file is no longer part of the *zip file on the Avaya software download website, but is available as a standalone download. If you already have such a file because you downloaded it for a previous release of the 4620, installing the standalone file will overwrite the original file.*

NOTE The same 46xxsettings.scr file is used by the 4620 and the 4630/4630SW IP Telephones.

In Table 4-7, parameters shown with a *Mandatory* status must be accurate and non-null for the application to work. Parameters with an *Optional* status may be changed to suit your environment; if they are not changed, the defaults will be used.

Table 4-7. 4620 IP Telephone Customizable System Parameters

Parameter Name	Default Value	Status	Description and Value Range
General User Parameters:			
SYSLANG	"English"	Optional (and can be user-specified)	Language of the 4620 user interface, in ASCII (independent of the MultiVantage™ message language). Choices are English, Deutsche, Espanol, Francais, Italiano, Nederlands, Portugues and Katakana (Japanese).
OPSTAT	1	Optional	Options status flag. When set to 1, the user can invoke any or all of the user options provided with the 4620 IP Telephone (see the *4620 IP Telephone User's Guide, Issue 1.8*). When set to 0, the user cannot invoke any option except those that are view-only; the user cannot change any setting.

Table 4-7. 4620 IP Telephone Customizable System Parameters—*Continued*

Parameter Name	Default Value	Status	Description and Value Range
Web Access Application Parameters:			
WMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application.
WMLPROXY	" " (Null)	Optional	Text string containing the IP address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the web pages to be accessed by the user are all on your organization's intranet.
WMLEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains, separated by commas, up to a total of 127 ASCII characters. This parameter is optional if the web pages to be accessed by the user are all on your organization's intranet. If WMLPROXY is null, the value of this parameter is ignored.
WMLPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if the web pages to be accessed by the user are all on your organization's intranet. If WMLPROXY is null, the value of this parameter is ignored.
WMLCODING	ASCII	Optional	Text string containing the coding to be used for characters entered in forms on web pages. Besides the default, other supported values include "Latin 1" and "Unicode". Note that "Unicode" includes support only for the Latin characters of Unicode.
Backup/Restore Parameters			
FTPSRVR	" " (Null)	Mandatory (but can be user-specified)	Text string containing the 4-octet IP address for the FTP server to be used for storage and retrieval of 4620 user information (see 4620 Backup/Restore, on page 4-41). Redundant with FTPSRVR listed as part of the 4630/ 4630SW Backup/Restore parameters.
FTPDIR	" " (Null)	Optional (and can be user-specified)	Path name for the directory on FTPSRVR used for storage and retrieval of user information. Redundant with FTPDIR listed as part of 4630/4630SW Backup/Restore parameters.

NOTE For assistance in developing local websites tailored to the 4620 IP Telephone's display, see Appendix C, Creating Websites for the 4620 IP Telephone.

4620 Backup/Restore

Backup/Restore automatically saves a phone's speed dial button labels and options/parameter settings (including local Feature Button labels). When the Automatic Backup option on a 4620 IP Telephone is set to "Yes" and the FTPSRVR is specified, the FTPSTOR command attempts to save all Speed Dial contents and all system options and (non-password) parameters to the FTP server (specified by FTPSRVR in the directory path specified by FTPDIR). Data is saved in an ASCII text file called "4620data.txt". The System Administrator may optionally specify FTPSRVR and/or FPTDIR via network administration, however, these values may also be specified by the phone's user, as covered in Chapter 6 of the *4620 IP Telephone User's Guide*. Automatic backup occurs whenever the user executes a Save command on a Speed Dial or Options/Parameter screen.

NOTE If your network includes both 4620 and 4630/4630SW IP Telephones, you need to specify **FTPSRVR** and **FTPDIR** once, and both telephones will use the same server and directory. They will, of course, store data in different files. In addition, users have the ability to specify alternative servers and directories (e.g., their own PCs) for backup and retrievals.

In addition to Speed Dial labels and associated phone numbers, the following options, settings and non-password parameters are saved during a backup:

Setting/Parameter Name	Type
Personalized Ring	Option
Redial	Option
Phone Screen on Answer	Option
Phone Screen on Calling	Option
Call Timer	Option
Message Display Rate	Option
Call Appearance Width	Option
Visual Alerting	Option
Call Log Enable	Option

Setting/Parameter Name	Type
4620 Contrast	Option
Display Language	Option
Automatic Backup	Option
FTP Server IP Address	Parameter
FTP Directory Path	Parameter
FTP User Name	Parameter

NOTE When the Options Status Flag, OPSTAT, is set to "0" (see Table 4-7), retrieving backed up data has no effect. This prevents a user from bypassing the administration of OPSTAT and changing options settings in the backup file.

Troubleshooting Guidelines

5

Introduction

This chapter describes problems that may occur during 4600 Series IP Telephone operation and possible ways of resolving these problems.

Error Conditions

Table 5-1, on page 5-2 identifies some of the possible operational problems that might be encountered after successful 4600 Series IP Telephone installation. Problems that might be encountered during installation, and how to conduct a Self-Test of the telephone, are discussed in the "Troubleshooting" chapter of the *4600 Series IP Telephone Installation Guide*. The *4630/ 4630SW IP Telephone User's Guide* and *4620 IP Telephone User's Guide* also contain guidance for users having problems with specific 4630/4630SW and 4620 applications, respectively.

NOTE Most of the problems reported by users of a 4600 Series IP Telephone are not likely to be problems with the telephone itself. More likely, the problems will be centered on the LAN, where Quality of Service, server administration, and other issues can impact end-user perception of IP Telephone performance.

Table 5-1. Some Error Conditions in Operation of 4600 Series IP Telephones

Condition		Cause/Resolution
The telephone continually reboots, or reboots continuously about every 15 minutes.		**CAUSE:** This is a firmware fault; the MAC address in memory is corrupted. **RESOLUTION:** The telephone must be returned to Avaya for repair.
The message light on the telephone turns on and off intermittently, but the telephone never registers.		**CAUSE:** This is a hardware fault. **RESOLUTION:** The telephone must be returned to Avaya for repair.
The telephone stops working in the middle of a call,	**AND** no lights are lit on the phone and the display is not lit.	**CAUSE:** Loss of power **RESOLUTION:** Check the connections between the telephone, the power supply, and the power jack. For example, verify that either static addressing was not used or that any changes to static addresses were entered correctly.
The telephone stops working in the middle of a call,	**AND** power to the telephone is fine (and the telephone may have gone through the restarting sequence).	**CAUSE:** Loss of path to Avaya media server, DHCP Lease expired, or DHCP server not available when telephone attempts to renegotiate DHCP lease. **RESOLUTION:** As above. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity, the usual "No Ethernet" message is not displayed.

Table 5-1. Some Error Conditions in Operation of 4600 Series IP Telephones—*Continued*

Condition		Cause/Resolution
The telephone had been working, but does not work now,	**AND** no lights are lit on the phone and the display is not lit.	**CAUSE:** Loss of power. **RESOLUTION:** Check the connections between the telephone, the power supply, and the power jack.
	AND power to the telephone is fine, but there is no dialtone. (Display might show “System Busy”.)	**CAUSE:** Loss of communication with the PBX switch **RESOLUTION:** Check LAN continuity from the PBX to the telephone (using ping or trace-route) and from the telephone to the PBX (by invoking a feature button). Verify the LAN administration has not changed for the TN799 or TN 2302AP boards or the LAN equipment (routers, servers, etc.) between the switch and the telephone. Verify no one has locally changed the telephone settings (by using the VIEW and ADDR codes, as described in the *4600 Series IP Telephone Installation Guide*). Verify the volume on the telephone is set high enough. Finally, conduct a self-test.
	AND the telephone was recently moved.	**CAUSE:** Loss of communication with the PBX. **RESOLUTION:** As above, but pay particular attention to the possibility that the telephone is being routed to a different DHCP server, or even a different PBX switch. If so, the new server or switch may need to be administered to support the telephone.
	AND the network was recently changed (servers upgraded or replaced, your Avaya media server switches, etc.).	**CAUSE:** Loss of communication with the PBX. **RESOLUTION:** As above.

Table 5-1. Some Error Conditions in Operation of 4600 Series IP Telephones—*Continued*

Condition		Cause/Resolution
The telephone works, but the audio quality is poor, specifically:	the user hears echo when speaking on a handset.	**CAUSE:** Echo from digital-to-analog conversion on your Avaya media server trunk. **RESOLUTION:** Verify which trunk is causing the echo, and swap the trunk's Trunk Termination parameter on the PBX.
	the user hears echo on a headset, but not on a handset.	**CAUSE:** Improper headset adapter. **RESOLUTION:** Replace adapter with Avaya's M12LU or 3412-HIC adapters. The M12LU is recommended, since it supports Automatic Gain Control.
	the user is on speakerphone and hears no echo, but the far end hears echo.	**CAUSE:** Room acoustics **RESOLUTION:** Ensure there are six inches or so of blank space to the right of the telephone. If that is insufficient, use the handset.
The telephone works, but the audio quality is poor, specifically:	the user experiences sudden silences (gaps in speech), static, clipped or garbled speech, etc.	**CAUSE:** Jitter, delay, dropped packets, etc. **RESOLUTION:** One or more Quality of Service (QoS) features should be implemented in the network (See Chapter 3 of the *4600 Series IP Telephone Installation Guide*). **CAUSE:** Improper (non-Category 5) wiring. **RESOLUTION:** Replace non-Category 5 wiring with Category 5 wiring.
The 4612 or 4624 IP Telephone works properly except the phone does not ring.		**CAUSE:** The Ringer Off (**RngOF**) softkey feature has been activated. **RESOLUTION:** Use the softkey **Menu** option to access the **RngOF** feature. A downward-pointing triangle means the Ringer is off. Ensure the triangle points up. Also, check the Volume setting on the telephone. Finally, do a Self-test on the telephone.

Table 5-1. Some Error Conditions in Operation of 4600 Series IP Telephones—*Continued*

Condition	Cause/Resolution
The telephone works properly except for the speaker.	**CAUSE:** The Speaker was turned off on the PBX. **RESOLUTION:** Administer the PBX to allow that station's speaker to operate. If that does not work, do a Self-test on the telephone.
The telephone works properly, except incoming DTMF tones are not received.	**CAUSE:** The TN2302AP board does not pass in-band DTMF tones. **RESOLUTION:** None; the board is operating as designed.
The telephone works properly, except sidetone DTMF is not heard.	**CAUSE:** PBX suppresses sidetone DTMF. **RESOLUTION:** On PBX administration, on the Change-System-Parameters screen, enable On-Hook Dialing. If the user has Hands-Free Answer (HFA) and answers the call on the telephone's speakerphone, then switches to the handset, pressing the dialpad buttons does not send DTMF tones. This is a known bug, and the only current resolution is to disable HFA.
Hands-Free Answer (HFA) is administered but the telephone did not automatically answer a call.	**CAUSE:** HFA only works if the telephone is idle. If a second call comes into the telephone while the first call is in progress (including ringing before the first call is answered), the second call is ignored. **RESOLUTION:** None.
The TFTP application terminates and asks for registration.	**CAUSE:** Non-Avaya shareware or freeware TFTP applications often cease operating to request registration. **RESOLUTION:** *Short-term:* Restart the application. *Long-term:* Register the product or replace it with an application that does not behave this way (for example, Avaya's TFTP application).

Table 5-1. Some Error Conditions in Operation of 4600 Series IP Telephones—*Continued*

Condition		Cause/Resolution
The TFTP script file is ignored or not used by the telephone		**CAUSE:** The telephone expects lines of the script file to terminate with a <Carriage Return><Line Feed>. Some UNIX applications only terminate lines with <Line Feed>. Editing the script file with a UNIX-based editor can strip <Carriage Return>s from the file, causing the entire file to be treated as a comment, and thus be ignored. **RESOLUTION:** Edit the script file with a Windows®-based editor, or another editor that does not strip out the <Carriage Return>.
	AND the TFTP server is a LINUX or UNIX system.	**CAUSE:** UNIX and LINUX systems use case-sensitive addressing and file labels. **RESOLUTION:** Verify the file names and path in the script file are accurately specified.
Power to the telephone is interrupted while the telephone is saving the application file **and** the TFTP application hangs.		**CAUSE:** The TFTP server hangs if power is interrupted while a telephone is saving the application file. **RESOLUTION:** Restart the TFTP server.
The DHCP server indicates the 4600 Series IP Telephone reports itself as a Token Ring device, and refuses to provide the telephone an address.		**CAUSE:** Early versions of the 4600 Series IP Telephones erroneously report being a Token Ring device. With most DHCP servers, this does not matter. Some LINUX servers, however, will refuse to issue addresses to Ethernet devices reporting to be Token Ring devices. **RESOLUTION:** Administer the DHCP server to delete all MAC and IP addresses associated with Lucent Technologies or Avaya, or allow the associated DHCP leases to expire.

Table 5-1. Some Error Conditions in Operation of 4600 Series IP Telephones—*Continued*

Condition	Cause/Resolution
The user indicates a 4620-specific or 4630/4630SW-specific application is not accessible.	**CAUSE:** The 46xxsettings script file is not pointed to accurately, or is not properly administered to allow the application. **RESOLUTION:** Assuming the user is meant to have that application, verify the 46xxsettings script file is properly specified for your system, including case (if your TFTP server is UNIX or LINUX) and extension. Then, verify all the relevant parameters (as indicated in Table 4-6, on page 4-34 and Table 4-7, on page 4-39, as appropriate) are accurately specified in the 46xxsettings file.

There are three areas where installers can troubleshoot problems before seeking assistance from the system or LAN administrator:

1. Check the wiring (power and Ethernet) for the following:
   - Whether all components are plugged in correctly.
   - Check LAN connectivity in both directions to all servers (DHCP, TFTP, Call Server). Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity the usual "No Ethernet" message is not displayed.
   - If the telephone is supposed to be powered from the LAN, ensure the LAN is properly administered and is compliant with IEEE 802.3af.
2. If you are using static addressing, do the following:
   - Use the View command to find the names of the files being used and verify that these filenames match those on the TFTP server. Check on the Avaya website to verify whether the correct files are being used.
   - Use the ADDR option to verify IP addresses.
   - Use the QOS option to verify QoS parameters.

   Refer to Chapter 3 of the *4600 Series IP Telephone Installation Guide*.
3. If the 4600 Series IP Telephone is not communicating with the system (DHCP, TFTP, or Call Server), make a note of the last message that was displayed and consult the system administrator.

The Reset Administrative Option

As indicated in some troubleshooting procedures, sometimes it is appropriate to reset the 4600 Series IP Telephone. Procedures on how to do so are printed below, and can also be found in Chapter 3 of the *4600 Series IP Telephone Installation Guide*. The following is the list of parameters, settings, etc., that are reset to default values (including "null" as applicable) when the Reset procedure is completed:

- All user-settable options (if applicable to the specific telephone).
- All user-created Speed DIal labels and associated telephone numbers (if applicable to the specific telephone).
- All user-generated administrable button labels (if applicable to the specific telephone).
- Registration extension and password.
- All values administered by local procedures, in accordance with Chapter 3 of the *4600 Series IP Telephone Installation Guide.*
- All values previously downloaded via DHCP or from a TFTP settings file (although, of course, these values are generally restored when the telephone goes through registration again after the reset.

Reset System Values

Use the following procedure to reset all system initialization values to the application software default values.

WARNING:

This procedure erases all static information, without any possibility of recovering the data.

1. While the phone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 7 3 7 3 8 # (**Mute R E S E T #**)

   NOTE Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630 and 4630SW IP Telephones do not have a dedicated **Hold** button; for all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button will also work.

   The following text is displayed left-justified at the top of the display:

   ```
   Reset values?
   *=no    #=yes
   ```

2. If you do not want to reset the system values, press ***** (no) and proceed to Step 4. Pressing the pound sign (#) to reset the system values displays a screen with the following prompt on the top line:

```
Are you sure?
*=no    #=yes
```

WARNING:

As soon as you press the # button, all static information will be erased, without any possibility of recovering the data.

3. Press the ***** button to continue without resetting the values and proceed to Step 4.
Or, press the # button to reset values to their defaults.

   The following text is displayed left-justified at the top of the display while the system values are reset to defaults:

```
Resetting
values.
```

   The telephone resets from the beginning of registration, which takes a few minutes.

4. If you do not reset the phone, the following prompt displays:

```
Restart phone?
*=no    #=yes
```

5. Press the ***** key to terminate the procedure without restarting the telephone, otherwise, press # and follow the Restart procedure directly below.

Restart the Telephone

Use the following procedure to restart the telephone.

1. While the phone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 7 3 7 3 8 # (**Mute R E S E T #**)

   NOTE Press the **Mute** button momentarily. Do not press this button while pressing other keys/buttons. The 4630 and 4630SW IP Telephones do not have a dedicated **Hold** button; for all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button will also work.

   The following text is displayed left-justified at the top of the display:

```
Reset values?
*=no    #=yes
```

2. Press the # button to reset values to their defaults, or ***** to continue.

   If you press the # button, the following text is displayed left-justified at the top of the display while the system values are reset to defaults:

   ```
   Resetting
   values.
   ```

   Once the system values are reset, the following prompt is displayed:

   ```
   Restart phone?
   *=no    #=yes
   ```

3. Press the ***** key to terminate the procedure without restarting the telephone.

   Press the # key to restart the telephone.

   The remainder of the procedure depends on the status of the boot and application files. Refer to Appendix A of the *4600 Series IP Telephone Installation Guide*.

The View Administration Option

If you are using static addressing and encounter problems, use the following procedure to verify the current values of system parameters and file versions.

NOTES

- Also use the ADDR option to view IP addresses (see "Static Addressing Installation" in Chapter 3 of *4600 Series IP Telephone Installation Guide*). These may have been entered incorrectly*. Verify whether you were provided with correct IP addresses.*
- If PROCPSWD has been administered as indicated in Server Administration, on page 4-1, you need to type the Local Procedure password after pressing **Mute** and before pressing V I E W.

1. While the phone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone:

   Mute 8 4 3 9 # (**Mute V I E W #**)

   NOTE Press the **Mute** key momentarily. Do not press this key while pressing other keys. The 4630 IP Telephone does not have a dedicated **Hold** button; for all other 4600 Series IP Telephones, pressing the **Hold** button instead of the **Mute** button will also work.

   The following text displays left-justified at the top of the display:

   ```
   View settings
   *=next   #=exit
   ```

2. Press the ***** button at any time during viewing to display the next name and system value pair from the list below, returning to the first pair after the last pair has been displayed.

   Press the # button at any time during viewing to terminate the procedure and restore the user interface to its previous state.

   The names and values are displayed in the following order:

Table 5-2. Parameter Values

Name	System Value	Format
Model	**46ccDccc**	up to 8 ASCII graphics characters
Market	**domestic** **export**	Only one value displays
Phone SN	**ccccccccccc** **cccccccc**	Phone Serial Number, up to 18 ASCII graphic characters
PWB SN	**ccccccccccc** **cccccccc**	Printed Wiring Board (circuit board) Serial Number, up to 18 ASCII graphic characters
PWB comcode	**ccccccccc**	9 ASCII numbered characters
MAC address	**00:60:1D:hh:hh:hh**	Each octet of the MAC address displays as a pair of hexadecimal numbers.
	filename1.exe	up to 16 ASCII graphic characters.
	filename2.exe	Out of the box, there will be only one **filename.exe**. After installation, there should be two filenames. If there is only one, installation has failed. Verify the problem, and then re-install the telephone.

Error Messages

The 4600 Series IP Telephones issue messages in English only. The IP Telephones also display messages from the switch, which outside the United States may issue messages in the local language.

Table 5-3. Possible Error Messages During Installation or Operation of 4600 Series IP Telephones

Error Message	Cause/Resolution
During Installation	
Checksum error	**CAUSE:** Downloaded application file was not downloaded or saved correctly. **RESOLUTION:** The telephone automatically resets and attempts to re-initialize.
DHCP: CONFLICT * to program	**CAUSE:** At least one of the IP address offered by the DHCP server conflicts with another address. **RESOLUTION:** Review DHCP server administration to identify duplicate IP address(es)
Discovering...	**CAUSE:** The telephone is seeking a gatekeeper on the call server, using its administered gatekeeper list. **RESOLUTION:** Wait for a valid registration to occur, or press # to interrupt the search and re-initialize manual or DHCP/TFTP procedures.
File too large Cannot save file	**CAUSE:** The telephone does not have sufficient room to store the downloaded file. **RESOLUTION:** Verify the proper filename is administered in the TFTP script file, and that the proper application file is located in the appropriate location on the TFTP server.
Gateway Error	**CAUSE:** DEFINITY Release 8.4 does not have an H.323 station extension for this telephone. **RESOLUTION:** On the station administration screen, ensure the DCP set being aliased for this IP telephone has an H.323 station extension administered, in accordance with switch administration instructions.
Hardware failure	**CAUSE:** Hardware failure prevented downloading of application file, **RESOLUTION:** Replace telephone.
IP Address in use by another	**CAUSE:** The telephone has detected an IP address conflict. **RESOLUTION:** Verify administration to identify duplicate IP address(es).

Table 5-3. Possible Error Messages During Installation or Operation of 4600 Series IP Telephones—*Continued*

Error Message	Cause/Resolution
No Ethernet	**CAUSE:** When first plugged in, the IP Telephone is unable to communicate with the Ethernet. **RESOLUTION:** Verify the connection to the Ethernet jack, verify the jack is Category 5, etc. Note that if the telephone is attached to a 30A switched hub, upon loss of Ethernet connectivity, the usual “No Ethernet” message is not displayed.
No file server address	**CAUSE:** The TFTP server IP address in the IP telephone’s memory is all zeroes. **RESOLUTION:** Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the TFTP server, or administer the telephone locally using the ADDR option as detailed in the *4600 Series IP Telephone Installation Guide*.
System busy	**CAUSE:** Most likely, the number of IP endpoints on the Avaya media server is already at maximum, Less likely, network resource is unavailable. **RESOLUTION:** The telephone was attempting to access a network resource (DHCP server, TFTP server, or the Avaya media server) and was not successful. The resource being called upon should be checked for its availability. If it appears operational and properly linked to the network, verify addressing is accurate and a communication path exists in both directions between the telephone and the resource.
System Error	**CAUSE:** The Avaya media server has an unspecified problem. **RESOLUTION:** Consult your Avaya media server administration and troubleshooting documentation.
During Registration	
Extension error	**CAUSE:** An invalid Avaya media server Registration extension has been entered. **RESOLUTION:** Re-enter the extension if mis-entered initially. If appropriate, verify proper extension with respect to switch administration.
Extension in use	**CAUSE:** The specified extension is already in use, according to the Avaya media server. **RESOLUTION:** Wait a few minutes, and try again. This will work for the case when the extension is correctly administered, but service was interrupted and the Avaya media server is not yet aware of that fact. Otherwise, verify proper extension with respect to switch administration.

Table 5-3. Possible Error Messages During Installation or Operation of 4600 Series IP Telephones—*Continued*

Error Message	Cause/Resolution
Failed to set phone IP address	**CAUSE:** The 4600 Series Telephone was originally installed on one switch with Static Addressing, and has subsequently been installed on another switch with an active DHCP server assigning dynamic IP addresses. **RESOLUTION:** Reset the telephone.
Incompatible	**CAUSE:** This release of the Avaya media server does not support the current version of the IP Telephone. **RESOLUTION:** Upgrade to the current version of Avaya media server software.
Message light blinks on and off, and the telephone did not complete registration.	**CAUSE:** The telephone has a hardware fault. **RESOLUTION:** Replace the telephone.
Password Error	**CAUSE:** An invalid PBX Registration password has been entered. **RESOLUTION:** Re-enter the password if mis-entered initially. If appropriate, verify proper password with respect to switch administration.
Resource Error	**CAUSE:** The Avaya media server rejects the registration request. **RESOLUTION:** Verify your Avaya media server administration to ensure the telephone's proper IP address, extension, and password are being used.
Timeout Error	**CAUSE:** Protocol timeout error. **RESOLUTION:** Retry. If failure continues, check network congestion, addresses, etc. to identify cause of timeout.
Undefined Error	**CAUSE:** An error has occurred without an identifiable cause. **RESOLUTION:** Conduct self-test, restart the telephone, and if no other cause becomes evident, replace the telephone.
Wrong Set Type	**CAUSE:** The Avaya media server does not recognize the set type. **RESOLUTION:** Ensure the Avaya media server is properly administered to expect the appropriate telephones for the IP address and extension.

Table 5-4. Possible Error Messages During 4620/4630/4630SW Backup/Restore

Error Message	Cause/Resolution
Current options and Speed Dial entries have not yet been backed up.	**CAUSE:** An attempt to save the current options and speed dial entries on the FTP server has not yet been made or is in progress. **RESOLUTION:** Wait for a message stating that backup was successful.
The FTP Server Name is not known. Please check the FTP Server IP Address	**CAUSE:** Invalid or missing Server name. **RESOLUTION:** Verify the FTPSRVR address is the File Server to which backup data should be saved. Verify that the FTPDIR value is the correct directory path for that File Server.
The FTP Server has not yet responded, so backup has not yet succeeded.	**CAUSE:** The FTP Server has not responded to the attempt to backup/restore. **RESOLUTION:** Try again, verify the FTP server address, verify the FTP server is online, and/or verify the network connectivity.
The FTP Server has denied access. Please check FTP Setup parameters.	**CAUSE:** The FTP Server has reported that it did not store data. **RESOLUTION:** Verify the FTP server setup parameters, as indicated on the FTP Setup Parameters screen (see “FTP Setup” in Chapter 8 of the *4630/4630SW IP Telephone User’s Guide)*.
The FTP Server was unable to store the backup file.	**CAUSE:** The FTP Server has reported that it could not store the data. **RESOLUTION:** Verify administration and available capacity/filespace on the FTP Server.

Appendix A: Avaya - 46xx IP Telephone MIB

A

Avaya - 46xx IP Telephone MIB

The custom Management Information Base (MIB) is available in *.txt format for free download at http://www.avaya.com/support. Follow these links: **Telephones and End User Devices**, then **4600 Series IP Telephones**, then **Product Documentation**.

Appendix B: Creating Websites for the 4630/4630SW IP Telephone

B

Introduction

This Appendix describes the capabilities and limitations of the web browser in the 4630/4630SW IP Telephone and provides suggestions for designing websites for viewing on the 4630/4630SW. It is intended for 4630/4630SW IP Telephone Web Browser [web page] designers, and assumes readers are familiar with HTML, Style Sheets, and ECMAScript.

This Appendix serves two primary functions. It:

- Presents the technologies that have been implemented in the 4630/4630SW IP Telephone Web Access application, including any limitations or non-standard implementations, and
- Provides a suggested model for developing effective web pages to be viewed in the browser.

This Appendix is not intended to provide technical details on setting up a web server, nor does it provide information on web server technologies. Finally, this document is not intended to provide an introduction to web browser protocols or technologies.

NOTES

- A link to sites where HTML templates are available for customizing can be found on the Avaya website.
- Any subsequent reference to the 4630 IP Telephone in this Appendix applies equally to the 4630SW IP Telephone.

General Background

The 4630 IP Telephone display is a quarter VGA (320 pixels wide by 240 pixels high, 256 colors supported) display.

The data types and other features supported in the browser include:

- HTML 4.0
- Cascading Style Sheets (CSS), Levels 1 and 2
- Document Object Model (DOM) Level 1
- Images: GIF and JPEG
- ECMAScript (JavaScript) 1.4
- HTTP 1.1
- Secure Sockets Layer (SSL) 3.0
- Cookies

Browser Features and Behavior

This section presents the technologies that have been implemented in the 4630 IP Telephone Web Access application, along with any limitations or non-standard implementations. Since style sheets have become the preferred mechanism for controlling web page appearance and have made obsolete most attribute specifications with tags, the majority of attributes for tags were not tried. The attributes that were tested were those of real interest to specific tags. The browser is HTML 4.0 compliant, with a few minor differences as noted below.

NOTE In the sub-sections that follow, comments specific to the 4630 IP Telephone and its browser are shown in italics.

Document Skeleton

Certain tags define the basic framework of an HTML document. While most browsers are normally good at dealing with missing tags, when style sheets are applied it is essential that the tag structures be followed. Even ignoring style sheets, it is considered good style to follow the HTML rules. The following tags make up the basic skeleton of an HTML document:

- <html> indicates the start of an HTML document.
- <head> indicates the start of an HTML document's header. Title, meta definitions, ECMAScript function definition, document level style sheet definition, and external style sheet inclusion are all done in the header section.
- <title> sets the title of the document. Normally this is shown in the frame of the browser window. *On the phone, the title is shown in the Top Line Information Display Area.*

- <body> indicates the start of the body of an HTML document. The rest of the document will be embedded between the start and end <body> tags.
- <meta> is used to add additional information about an HTML page. *This is typically used by web walking tools, is of little use in browsers, and has no effect on the phone.*

Content-Based Style

Content-based tags deal with identifying words, phrases or chunks of text, or images as having a specific meaning or context. The intent of content-based tags is not to show physically marked text. However, it is not wrong for a browser to show content-based text in a distinct style, such as font style.

Each content-based tag is shown with a brief description, and any physical effects imposed by the browser.

- <abbr> indicates an abbreviation. *Using this tag has no effect.*
- <address> indicates an address. *Using this tag has no effect.*
- <acronym> indicates an acronym. *The enclosed text is shown in an italic font.*
- <cite> indicates a bibliographic citation or reference. *The enclosed text is shown in an italic font.*
- <code> indicates source code of a program. *The enclosed text is shown in a monospaced font.*
- <del> indicates deleted text. It is intended to show editorial markup. *The enclosed text is shown with a line through it.*
- <dfn> indicates a definition for a term. This is normally used with the first appearance of a term in a document. *The enclosed text is shown in an italic font.*
- indicates emphasis on a string of text. This is the contextual equivalent of using the <i> (italic) tag. *The enclosed text is shown in an italic font.*
- <ins> indicates inserted text. It is intended to show editorial markup. *The enclosed text is shown underlined.*
- <kbd> indicates keyboard input. This is similar to the <code> tag, but with a different contextual intent. *The enclosed text is shown in a monospaced font.*
- <samp> indicates literal text. *The enclosed text is shown in a monospaced font.*
- indicates emphasis on some text, but in a stronger contextual sense than the tag. This is the contextual equivalent of using the <b> (bold) tag. *The enclosed text is shown in a bold font.*
- <var> indicates source code variables. This is similar to the <code> tag, but with a different contextual intent. *The enclosed text is shown in an italic font.*

Logical Style

Tags that control logical style provide a similar functionality to those that control content-based style, but they have no implicit visual characteristics or contextual meaning. Instead, they only provide a means of invoking a style sheet. These tags, like all others, may have an ID and class attribute set. Using style sheet rules for these class names and IDs allows the designer to provide decoration, font, and color styles to each section. Thus, these tags may be considered to be designer-defined content-based tags:

- indicates a division. A newline is inserted between the previous text and the text following the tag. No physical changes are noticeable, except those implemented in style sheets.
- indicates a spanned section of text is placed immediately after the text preceding the tag with a newline. No physical changes are noticeable, except those implemented in style sheets.

Physical Style

Physical tags are effectively the opposite of content-based tags. The text in a physical tag may have no meaning whatsoever, outside of what the designer intended. These tags show text in a distinct style. Physical tags typically affect font style.

Each physical style tag is shown below with a brief description, and any physical effects imposed by the browser.

- <b> indicates that the text should appear in a bold font weight.
- <big> indicates that the text should appear one point size larger than the current text.
- <i> indicates that the text should appear in an italic font.
- <small> indicates that the text should appear one point size smaller than the current text.
- <sub> indicates that the text should appear as a subscript to the current text. The text is shown one point size smaller.
- <sup> indicates that the text should appear as a superscript to the current text. The text is shown one point size smaller.
- <tt> indicates that the text should appear as teletype text. The text is shown in a monospaced typeface font.

Physical Spacing and Layout

Physical spacing and layout tags define the basic structure of a document. Headings, paragraphs, tables and lists all provide some basic physical and logical layout to a page.

Each spacing and layout tag is shown with a brief description, and any unusual behavior is described.

- <p> indicates the start of a new paragraph. A blank line is inserted between previous text and text following the <p> tag.
-
 indicates that a breakpoint should be inserted. A newline is inserted between previous text and text following the <br> tag.
- <pre> indicates that the following text should have no formatting rules applied to it. This implies that no wrapping will be applied to this text, which may result in a horizontal scrollbar being added to view the text.
- <hr> indicates that a newline and a horizontal rule (line) should be inserted between the previous text and text following the <hr> tag.
- <blockquote> indicates that the following text is a quote, and should be offset in some way. The embedded text is shown with newlines before and after the text, and spacing to the left and right. Within that "block" of text, normal wrapping rules are applied.
- <q> indicates that the following text is a short quote, and should be shown in double-quotes (according to documentation). This text appears as normal text, with no physical identifying indications.
- <h1> - <h6> indicate heading sections. Each level is one point smaller than the previous level, with <h1> being the largest.

The section titled Maintaining Context, on page B-12 contains design guidelines for maintaining user context.

Lists and Tables

For presentation of data in a logical format, lists and tables are two of the more important sets of tags. Since space is at a premium in the browser, tables should be used with discretion. While they provide sets of text, which are easy for the eye to process, they can quickly become cumbersome if misused in this browser. Both width and height are limited, so the data provided in the table cells should be short pieces of text. Beyond that, the page designer should come up with a different model for presenting the data, possibly using lists and divisions.

Lists

- starts an ordered list. This provides a list with some type of numbering: upper-case letters, lower-case letters, digits, upper-case roman numerals, lower-case roman numerals. Setting the type attribute is ignored in the browser.
- starts an unordered list. This provides a list with bullets to the left of each item.
- adds an item to an ordered or unordered list.
- <dl> starts a definition list. This is a list with two fields per list item. The first is a term and the second is the term's definition.
- <dt> adds a new definition term to a definition list.
- <dd> adds a new term definition to a definition list.

Tables

The new HTML 4.0 table tags, <thead>, <tbody> and <tfoot> are all implemented. These tags are intended primarily to allow printed pages to have headers and footers appear on each page, when the table is longer than a single page. Since the 4630 IP Telephone Web Browser does not provide the ability to print, it is recommended that these tags not be used.

- <table> starts a table layout.
- <caption> adds a caption to a table. The align attribute allows a caption to be placed above or below the table. This attribute has no effect in the phone.
- <tr> adds a new table row to a table.
- <th> adds a header for some column(s) of a table.
- <td> adds a piece of data for some row(s) and column(s) of a table.
- <thead> defines a set of table header rows. The intent of this tag is to provide a set of header rows for each printed page. While viewing the page in a browser, the header has no more effect than the <th> tag. What it does provide for the designer is a more logical breakout of the data. It is easy to recognize the header area of the table since it is set between the <thead> start and end tags.
- <tbody> defines the main body of a table, when used in conjunction with the <thead> and <tfoot> tags.
- <tfoot> defines a footer for a table. This tag may contain multiple rows. Like the <thead> tag, the intent of this tag is to provide a set of footer rows for each printed page. Viewing the page in a browser has no additional effect. And like the <thead> tag, this tag provides a logical breakout of the data for the designer.
- <colgroup> defines a column group. It may be used as a single definition of identical columns or as a container for dissimilar columns. The span attribute defines what columns are parts of each group.
- <col> controls the appearance of one or more columns within a column group.

Images

The 4630 IP Telephone Web Browser handles both GIF and JPEG image formats. No other image formats, included animated GIFs, are supported. Note that images take up a large amount of memory (compared to text) and updating the display can be an issue; therefore, it is recommended that images be kept to a minimum.

The image tags that may be used on the browser are as follows:

- <img> displays an image.
- <map> display a client-side image. Client-side images have shaped regions called areas. These areas are tied to URLs or ECMAScript functions. When an area in a region is clicked, the ECMAScript function is executed.
- <area> defines an area in a <map> image. Each area uses the href attribute to define a URL to jump to, or some ECMAScript to execute, when the mouse is clicked on that area.

See the Design Guidelines, on page B-10 for information on displaying images.

Links

As of Release 1.8, the 4630/4630SW IP Telephones support dialing from hyperlinks. Specifically, if the value of the HREF attribute for a given link is of the form “tel:*nnnnn*” or “javascript:dial(‘*nnnnn’)”,* when that link is selected, the characters *nnnnn* are passed to the 4630/4630SW Phone application for direct dialing.

Hyperlinks are the heart of the web browser’s power. The link is what allows the user to click on some text or an image to jump to another web site, another page within this site, or another area in this page. Although URLs allow various protocols to be used, only http and https should be used for the 4630 IP Telephone Web Browser.

- <a> specifies the full or relative URL for a hyperlink. When using the target attribute, the _blank name should never be used. With the exception of frames, the 4630 IP Telephone Web Browser is not intended to be a multi-window browser. Thus, if a page attempts to reference a new, non-frame window, the browser will become confused and a reboot will be necessary.
- <base> defines the default target to be used in all <a> tags. This is done by setting the target attribute of the <base> tag. If the target attribute has been set in the <a> tag, the <base> tag value is ignored.

The use of the target attribute with the Web Access Application is strongly discouraged because the application supports a single window for browsing. The use of the target attribute may cause the browser software to create a new window that is outside of the Web Access Application's control.

Frames

Frames allow multiple windows to be created on the browser's base window. The browser is effectively split up into multiple areas. Each frame may be given a name or ID. Using the target attribute of the <a> tag, a web page may be displayed in another frame.

Although frames behave as defined, the small size of the screen makes them impractical to use. Just like tables, frames take up too much room on the display. One could, though, take advantage of frames by having a small "table of contents" frame with images for links. In general, however, use of frames is strongly discouraged.

- <frameset> defines an area for a set of frames.
- <frame> defines a single frame in a frameset.
- <iframe> defines an in-line frame. More detail
- <noframes> provides a fallback for browsers that don't handle frames. If the designer intends to use frames and make these pages available to phone, this tag should certainly be employed.

See the Design Guidelines, on page B-10 for information on displaying frames.

Forms

HTML forms provide the user the ability to enter data into a web browser. This data can then be passed on the web server for processing. It is difficult to predict what web designers might have in mind for the 4630 IP Telephone Web Browser. However, all forms-related tags have been verified, and the results are presented here.

- <form> defines the basic input form, and defines the action to be performed when the submit button is selected, via the action attribute.
- <input> defines most user input. The type attribute defines the type of input to be used. The <button> tag was created to replace type values of button, reset and submit, in a cleaner, more flexible way. Other type values available are checkbox, hidden, image, password, radio, and text. The type value file is useless in the context of this browser, since the intent of this control is to allow the user to select a file on their local disk.
- <button> defines a button that the user may select. This behaves much like the <input type=button> tag, except that the physical appearance is three-dimensional and any text, image, or combination, may be displayed in the button.
- <fieldset> encapsulates a section of a form's contents to create a group of related form controls. The phone's browser puts a simple box around the fieldset.
- <label> associates a relationship between a form control and one or more text labels. Labels may be tied to form controls by the for attribute in the label and the id attribute in the form control. They may also be tied by embedding the form control inside the <label> tag (for example, <label>Name: <input type=text id=name></label>).
- ·<legend> gives a label to a <fieldset> tag. This label appears at the top of the fieldset section of the form, with a line separating the legend from the rest of the fieldset.
- <optgroup> provides nested, cascading menus to the user. This doesn't seem to work.

- <option> defines the values available in a <select> scrolling list or drop-down menu.
- <select> defines scrolling lists and drop-down menus.
- <textarea> provides free-form user input and display. This provides a scrolled text area for the user to read or type text.

Character Entities

As with any syntactic language, HTML has certain characters that have special meaning. The two most obvious of these characters are the < and > symbols, which surround all tags. These characters cannot be typed in directly if the designer's intent is to display these characters. Thus, all characters that can be displayed in a web browser have numeric values assigned to them. In addition, many of these characters have names also assigned. The numeric values are entered into the source web page as &#nnn; where nnn is some 3 digit value. For example, the < symbol is entered as '<'. Name values are entered into the source web page as &name; where name is the name associated with this character. Again, using the < symbol, this would be entered as '<'. The set of characters defined by the World Wide Web Consortium are fully supported in the browser in conformance with the standard.

Colors

The browser supports 256 colors. Colors may be specified by name, RGB percentages or RGB raw numbers. The HTML and CSS specifications suggest 16 named colors. The 4630 IP Telephone browser recognizes these color names, which are: aqua, black, blue, fuchsia, gray, green, lime, maroon, navy, olive, purple, red, silver, teal, white, and yellow. Beyond these 16 well-known names, it is recommended that RGB percentages or raw numbers be used for specifying colors.

Fonts

Font specifications are one of the most important styles that may be applied to a web browser. Because of the size of the screen on the 4630 IP Telephone, the browser has only a single font available for use. Font weights, such as normal and bold, are supported, although finer values, such as lighter and bolder are not. Normal and Italic font styles are also supported. Font sizes are also supported, specified by either percentages or raw numbers can be used. However, percentages below 50% all appear as the same size.

Although some problems were found with font specifications, given the size and resolution of the screen, fonts behave reasonably well. The only major problem found is the inability to specify font families.

See the Design Guidelines, on page B-10 for information on displaying images.

Cookies

Cookies can be a useful feature in maintaining the state of a user when interacting with a web site. HTTP provides no state information, such as when or how often a user has visited a site. Cookies allow web sites to track this information by storing a simple set of values on the browser for the current session. Normally, browsers also provide the ability to save cookies to disk, so this information may be retained between sessions. However, the 4630 IP Telephone browser has no such ability to save any data between sessions. Cookies do behave well within the realm of the current session, and may be employed if desired. The 4630 IP Telephone has a maximum of 8Kilobytes of data available for cookie storage.

Design Guidelines

This section presents guidelines for developing a good model that effectively presents web pages to be viewed on the 4630 IP Telephone Browser. The biggest challenge in designing pages for this browser is the limited amount of space available for viewing the pages. The 4630 IP Telephone screen is a ¼ VGA display. Part of that screen is lost to the browser by the main controls of the 4630 IP Telephone. Thus, page layout must be done effectively and efficiently so as to avoid causing more space to be lost through additional screen controls such as scrollbars. Font sizing will make or break the usability of a page. A balance must be found between fitting as much text as is possible, and allowing users to read the text without straining their eyes.

Fixed-Width Objects

One of the primary functions of a web browser is to present text, wrapped at the right (or left when dealing with internationalization) border of the browser window. The browser always attempts to avoid adding a horizontal scrollbar. However, if fixed-width objects, such as tables and pre-formatted (<pre> tags) text are used, the browser makes wrapping a secondary priority to presenting the data exactly as the HTML dictated.

Web browsers do not resize themselves larger when scrollbars are added. Thus, if there are more lines of text than can fit in the height of the browser window, a vertical scrollbar is added. This now takes up some of the width of the browser, and less text displays on a single line. If text is wider than the width of the browser, a horizontal scrollbar is added. This now takes up some of the height of the browser, and fewer lines of text are displayed.

Given the small size of the browser, it is highly desirable to avoid causing scrollbars to appear. Unless the amount of text shown in a page is kept to a bare minimum, it is unlikely that a vertical scrollbar will be avoided. However, avoiding fixed-width objects, or ensuring that the size of fixed-width is kept small, will gain some viewable space on the browser.

In general, if scrolling is a requirement, vertical scrolling is better perceived by users than horizontal scrolling.

Images

The use of images in a web page is always a concern. For example, a page with many images can cause downloading to be slow. While this is still a concern in the phone, the size of an image has a much greater effect. Memory in the browser, and in the phone in general, is limited. Each image will use a sizable amount of memory, and the browser may become overwhelmed. An image should only be used if it is essential to a page.

Images also fall into the realm of fixed-width objects. All images should be checked to verify that they don't cause a horizontal scrollbar to be added. An image may be scaled down by the browser, by setting the width and height attributes of the <img> tag. The designer may instead choose to scale the images when setting up the web site. This avoids forcing the browser to deal with the sizing (using the width and height attributes scales the image after it is downloaded by the browser) and speeds up downloading of the images. Finally, reducing the size of the image reduces the amount of memory used.

Animated GIF images are a bad idea since they use up quite a bit of memory. Additionally, because of the persistence of the LCD screen, animated images tend to smear in the browser and lose their effectiveness. Hence, animated GIFs are considered "not supported" with this phone.

Frames

While frames provide a useful method of browsing a series of pages (via a contents frame and a document text frame), they also use up real estate, just like scrollbars. Even if the frame decorations were all turned off, the frame containing the majority of the document text now suffers the problems discussed above; the width of the frame is smaller, and the chances of adding a horizontal scrollbar have increased. Additionally, a single line of text will have fewer characters viewable, and the page becomes even more difficult to read and comprehend. Using simple navigation buttons at the top and bottom of the page, or even at the top and bottom of each section should make up for the missing contents frame.

The interaction between frames and scrollbars is another important area of concern. While most browsers manage scrolling within each frame independently, the 4630 Web Access Application only scrolls the entire (single) window. This moves the user's view of the frames as a whole, but it does not scroll any of the data in individual frames. There will likely be data in frames that can never be seen.

The combined problems of minimal screen real estate and the scrolling issues really makes frames something simply to avoid.

Fonts

Font size is a major concern in the browser. Without designer intervention, the browser displays text as if it were running on a PC in a normal width and height display. This means that the fonts shown would appear huge relative to the screen size. As a result, only seven lines of text will be viewed in the browser when no font sizing is applied. Additionally, only about 25 characters would be viewed per line. This would generally be unusable from a practical point of view.

To make the browser usable, some form of font sizing should be performed to allow a reasonable amount of text to be viewed on one screen. Ideally, font sizing should be done in a single external style sheet, and all pages should reference this style sheet. Setting font sizes in document-level style sheets, or even worse, in in-line style sheets or <font> tags, makes it very difficult for the designer to update font changes, and runs the risk of failing to make the change everywhere. By using a single external style sheet, consistency in the pages is managed.

Defining fonts may be done in a static external style sheet or by dynamically generating a style sheet using some form of server-side application, such as a CGI script or a Java servlet. Using dynamic generation of a style sheet allows the server to decide, per user, what font size to use. This in turn allows the user to notify the server to change the font size. All HTML pages would have an external style sheet reference, which is another server-side executable. This executable would dynamically generate font information based on the cookie, form component or configuration value, relative to the IP address of the phone.

Using a static external style sheet makes page development and testing much easier, since how it appears to the designer would be how it appears to the reader. Allowing the user to choose a font size forces more work on the designer to verify that all fixed size items appear acceptably

Maintaining Context

Given the small working area, it is easy for the user to become lost. Headings will often not be in view, and the user, if distracted by other work, can lose their sense of context. Style sheets may be used to help maintain this sense of context through color. The and tags are intended to provide page designer-defined content-based style. By defining classes of tags with various colors and border styles, the designer may provide additional information. It is important to bear in mind that a significant number of people suffer from some form of color blindness. Thus, it may be necessary to design pages both with and without using color styles.

User Interaction

As discussed above, HTML forms work reasonably well in the browser. However, due to the limitations of the phone as an input device, keyboard input can be difficult. A complete keyboard is made available based on the context of mouse selection. When a text input control is on-screen, the user simply needs to click on the input control. The keyboard appears, with the browser thrown into a small scrolling area. The input control is roughly centered in the scrolling area. The user may then press the software keys and the text is shown in the input control. Simply pressing the done button dismisses the keyboard, and the input control shows the newly typed text. While this interaction technically works fine, from a user perspective, it can be difficult to type a large amount of text. Thus, unless user input is absolutely necessary, it should be avoided. When necessary, user input should be kept to a minimum.

Appendix C: Creating Websites for the 4620 IP Telephone

C

Introduction

This Appendix describes the capabilities and limitations of the web browser in the 4620 IP Telephone and provides suggestions for designing websites for viewing on the 4620. It is intended for 4620 IP Telephone Web Browser (web page) designers, and assumes readers are somewhat familiar with WML.

This Appendix serves the following functions:

- Presents the portions of WML that have been implemented in the 4620 IP Telephone Web Access application, including any limitations or non-standard implementations
- Provides considerations for developing effective web pages to be viewed in the browser

This Appendix is not intended to provide technical details on setting up a web server, nor does it provide information on web server technologies. Finally, this document is not intended to provide an introduction to web browser protocols or technologies.

General Background

The 4620 Telephone has a 168 pixel-by-132 pixel four-gray scale LCD display. The area of the display available for presenting a WML web page to the user is 168 pixels across by 96 pixels in height, arranged in 6 rows each 16 pixels in height. In addition, the top row will display the web page title (if any) and the bottom row presents up to four softkey labels at one time, each a maximum of 6 characters, that are used for <do> tags.

The data types and other features supported in this browser include:

- WML 1.3
- HTTP 1.1

A chart at the end of this Appendix summarizes the more detailed information that follows.

NOTE Unsupported WML 1.3 tags will not be rendered and will not cause the browser to fail. Unknown tags and misspelled tags will cause an error message.

WML Document Skeleton

Certain tags define the basic framework of a WML document. The tags listed below make up the basic skeleton of a WML document, and are supported by the 4620 unless otherwise indicated.

- Common tag attributes: xml:lang, class, and id

  The attributes xml:lang, class and id are universal attributes associated with every WML element. The web browser will support these tags as follows:

Attribute	Comments
xml:lang	NOT SUPPORTED
class	NOT SUPPORTED
id	SUPPORTED

- <**wml**> tag - The <wml> tag defines a deck of cards and encloses all information the deck and is a required WML element. This tag must contain at least one <card> tag.
- <**head**> tag - The <head> tag is an optional WML tag containing information relating to the deck as a whole, including meta-data and access control elements. This tag is not supported.
- <**meta/**> tag - The optional <meta> tag is contained between multiple <head> tags. This tag gives values for the parameters that describe the content of the deck. This tag is not supported.
- <**card**> tag - A single WML file can contain multiple cards. This leads to the analogy - a "deck" of "cards" within a single WML file. A "card" is essentially the specification of one specific WML page. This is a mandatory tag.

The card element attributes supported by the web browser are as follows (unsupported attributes are indicated as such in the Comments column):

Attribute	Value(s)	Description	Comments
newcontext	true false	Re-initializes the browser context Default is "false"	Clears out the current WML browser context. This entails emptying the navigation stack history and clearing out all variables. NOT SUPPORTED
ordered	true false	Specifies the order of card content. When ordered is set to "true" the browser will display the content in a fixed order. When ordered is set to "false" the users will decide the order as they navigate between content. Default is "true"	Optional; sets a Boolean value that provides information on how the content of the current card is arranged. Used by the browser to organize the display presentation and layout. If set to true, content is organized in a linear sequence of elements (for example, a series of ordered or non-optional input elements). If set to false, content is in no natural order (for example, a series of unordered or optional input elements). The default is true. NOT SUPPORTED.
title	*cdata*	The title of the card	Can be used for title displays. SUPPORTED
onenterbackward	*url*	Occurs when the user navigates into a card using a “prev” task	SUPPORTED
onenterforward	*url*	Occurs when the user navigates into a card using a “go” task	SUPPORTED
ontimer	*url*	Occurs when a “timer” expires	SUPPORTED

- <**template**> tag - The <template> tag defines a template for all the cards in a deck. The "code" in the <template> tag is added to each card in the deck. Only one <template> tag for each deck may be specified. This tag can only contain <do> and <onevent> tags.

The **template** tag attributes supported by the 4620 web browser are as follows:

Attribute	Value(s)	Description	Comments
onenterbackward	*url*	Occurs when the user navigates into a card using a "prev" task	SUPPORTED
onenterforward	*url*	Occurs when the user navigates into a card using a "go" task	SUPPORTED
ontimer	*url*	Occurs when the "timer" expires	SUPPORTED

NOTE The implication for rendering WML pages is that the local environment will always override a global template for <do> types with the same name and type. If there is a onevent in the template and a *local* onevent of the same type, the local onevent takes precedence over the global one.

- <**access**> - The <access> tag limits access within the deck to certain cards. This tag is not supported.

Text Elements

- <**br**> tag - The <br> tag tells the browser to add a line break to the text at the point the element is written.
- <**p**> tag - The <p> tag specifies a paragraph of text with alignment and line wrapping properties. All text data must be contained inside this tag. Only <do> tags, wml and card elements can exist outside of the <p> tag. When rendered, this tag will cause subsequent text to begin on the next line.

Attribute	Value	Description	Comments
align	left right center	Aligns the paragraph. Default is “left”	SUPPORTED
mode	wrap nonwrap	Sets whether a paragraph should wrap lines or not	Since horizontal scrolling is not supported, all text lines are wrapped. WML pages with mode=nowrap are ignored, and the text will wrap. NOT SUPPORTED.

The following tags are not supported but the content inside the tags will be rendered as normal text:

- <**table**> tag - The <table> tag specifies a table. This tag is not supported.
- <**td**> tag - The <td> tag defines individual cell contents in each row of a defined table. This tag is not supported.
- <**tr**> tag - The <tr> tag defines each row of a defined table. This tag is not supported.

Text Formatting Tags

The following tags are not supported but the content inside the tags will be rendered as normal text:

- <**b**> tag - The <b> tag specifies bold text. This tag is not supported.
- <**big**> tag - The <big> tag specifies large font text. This tag is not supported.
- <**em**> tag - The tag specifies emphasized text. This tag is not supported.
- <**i**> tag - The <i> tag specifies italicized text. This tag is not supported.
- <**small**> tag - The <small> tag specifies text using a small font size. This tag is not supported.
- <**strong**> tag - The tag specifies strongly emphasized text. This tag is not supported.
- <**u**> tag - The <u> tag specifies underlined text. For the 4620 Web Access application, only links appear underlined. This tag is not supported.

Anchor Elements

- <**a**> tag - <a> elements define <go> tasks that require a URL link specification. All <a> tags will be rendered as underlined. All <a> nested tags (br, img) are supported. One anchors may be rendered is rendered per line. The user can select the link by pressing the left Feature Buttons associated with that display line.

Attribute	Value	Description	Comments
href	*url*	REQUIRED. Defines where to go when the user selects the link	SUPPORTED
title	*cdata*	Defines a text identifying the link	SUPPORTED
accesskey			NOT SUPPORTED

- <**anchor**> tag - <anchor> elements define <go> tasks that require a URL link specification. All anchors are rendered as underlined. All <anchor> nested tags (br, go, img, prev, and refresh) are supported. A maximum of 6 anchors may be rendered on the screen at one time. The user selects a link by using the Left Feature button associated with that display line.

Attribute	Value	Description	Comments
title	*cdata*	Defines a text identifying the link	SUPPORTED

Image Elements

- <**img**> tag - The <img> tag is used to place an image in the text flow. The 4620 supports the rendering of black-and-white Wireless Bitmap (WBMP) images, up to 152 pixels wide and 1536 pixels (96 lines of 16 pixels high each) high. Large images are not recommended. Images can be part of a link and can be selectable. At most, 10 images can be displayed per card.

Attribute	Value	Description	Comments
align	top middle bottom	Aligns the image	NOT SUPPORTED
alt	*cdata*	REQUIRED. Sets an alternate text to be displayed if the image is not displayed. If this is not supplied, either default text displays (if available) or the following message displays: “Image not displayed”.	SUPPORTED
height	*px* *(pixel)* %	Sets the height of the image	NOT SUPPORTED; the true height parameters will be determined by parsing the WBMP information.
hspace	*px* %	Sets white space to the left and right of the image	SUPPORTED; default is 1 pixel.
localsrc	cdata	Sets an alternate representation for the image	NOT SUPPORTED
src	url	REQUIRED. The path to the image. Must be a .wbmp file.	SUPPORTED
vspace	*px* %	Sets white space above and below the image	SUPPORTED; default is 1 pixel.
width	*px* %	Sets the width of the image	NOT SUPPORTED; the true width parameters will be determined by parsing the WBMP information.

Event Elements

- <**do**> tag - The <do> tag is a card-level user interface. It serves as a general mechanism for the user to activate a task, typically performed by the user clicking on a word or phrase in the display. A task is performed in response to an event. There are four tasks in WML: go, noop, prev, and refresh.

The mandatory *type* attribute provides information about the intent of the element, helping to improve processing. If the 4620 web browser does not recognize the specified type, (e.g., testing, experimental, and vendor specific types), the specified type is treated as unknown. The browser only renders WML 1.2 tags. Any other tags will cause an error and the user will receive an error statement "not a valid wml page".

Attribute	Value	Description	Comments
type	accept prev help reset options delete unknown x-* vnd.*	REQUIRED. Defines the type of the "do" element	SUPPORTED
label	cdata	Creates a label for the "do" element	Optional; creates a string label for the element. The 4620 browser imposes a six character limit. SUPPORTED
name	*mmtoken*	Defines a name for the "do" element	SUPPORTED
optional	true false	If set to true, the browser ignores this element. If set to false, the browser does not ignore this element. Default is "false"	Optional. SUPPORTED

Type	Description	Comments
accept	Acknowledgement of acceptance	SUPPORTED
delete	Delete item	SUPPORTED
help	Request for help	SUPPORTED
options	Options or additional operations	SUPPORTED
prev	Backward navigation	SUPPORTED
reset	Clearing or reset	SUPPORTED
X-*n or x-*n	Experimental	SUPPORTED, but treated as ‘unknown’

<**do**> tags are rendered as softkey labels on the bottom line of the 4620 display. <do> tags are specified per WML page and therefore are page context-sensitive. The eight “do” types are labeled either specifically in a WML page or by a browser-dependent label.

If no labels are given, then the “do” types will have the following default labels:

Type	Default Label if no label specified
accept	ACCEPT
delete	DELETE
help	HELP
options	OPTIONS
prev	BACK
reset	RELOAD
X-*n or x-*n	UNKNOWN
Vnd* Any mix of upper or lower cases	AVAYA (Available for future use, but currently UNKNOWN)

If no <do> tags have been specified, no softkeys will be displayed:

If one <do> tag is specified the following softkeys will be displayed:

1st DO			

If multiple <do> tags are specified, display them as follows:

1st DO	2nd DO	3rd DO	MORE

Page 1 Softkeys:

1st DO	2nd DO	3rd DO	MORE

Page 2 Softkeys:

4th DO	5th DO	Etc.	MORE

NOTE If more than one page of softkey labels are specified, pressing the MORE softkey automatically presents the user with the next page of labels. If the last page displays and the user presses the MORE softkey, the first page of labels is then displayed. As implied by the above, the softkey buttons are labeled in sequential order of the <do> tags.

- <**onevent**> tag - The onevent tag serves as a container for code that you wish to be executed automatically when one of the four intrinsic events occurs. The onevent element is said to bind (associate) the tasks (code) to the event for the element. The intrinsic event must be specified using the mandatory type attribute.

  For example, when a user presses the BACK softkey, instead of being routed to the previous screen, the user will be directed to another specified page because this tag carries out a onevent backward event.

The intrinsic events are:

Event	Permitted Tags	Description
onenterbackward	card or template	Occurs when a <prev> navigates back onto a card. SUPPORTED.
onenterforward	card or template	Occurs when a <go> navigates into a card. SUPPORTED
onpick	option	Occurs when an item is selected/unselected by a user. SUPPORTED
ontimer	card or template	Occurs when the time expires. SUPPORTED

The template element creates code that is inserted into all cards in a single deck. The nested tags are as follows, go, noop, prev, and refresh.

There are no visual implications for supporting the <onevent> tag.

Attribute	Value	Description	Comments
type	onenterbackward onenterforward onpick ontimer	REQUIRED. Specifies the type of the “onevent” element	SUPPORTED

- <**postfield**> tag - The postfield tag is used to set a name/value pair that can be transmitted to an origin server (source of the request) during a URL request. The name is set by the name attribute and must be a valid WML variable name. The value is set by the value attribute. There are no visual rendering implications with this tag.

Attribute	Value	Description	Comments
name	*cdata*	REQUIRED. The name of the field	SUPPORTED
value	*cdata*	REQUIRED. The value of the field	SUPPORTED

Task Elements

- <**go**> tag - The go element can contain one or more postfield elements. If the destination of a go element is a card within the same deck, all of the postfield elements will be ignored. The go element can also contain one or more setvar elements. Unlike postfield elements, there are no destination limitations on passing information contained in the setvar elements. The <go> nested tags (postfield and setvar) are supported.

Attribute	Value	Description	Comments
href	url	REQUIRED	SUPPORTED
accept-charset	Charset_list	A comma- or space-separated list of character encoding the server must be able to process. The default value is "unknown".	SUPPORTED
method	post get	Sets how to send the data to the server. Default method is get. When method="get", the data is sent as a request with*?data* appended to the URL. The disadvantage of get is that it can be used only for a limited amount of data; if you send sensitive information it will be displayed on the screen and saved in the web server's logs.With method="post", the data is sent as a request with the data sent in the body of the request. This method has no limit, and sensitive information is not visible.	SUPPORTED
sendreferer	true false	If set to true, the browser sends the URL of the current deck with the request, which allow servers to perform simple access control on decks, based on which decks are linking to them. Default is "false"	SUPPORTED

- <**noop**> tag - The noop tag dictates that no operation should be done. This tag can be used on the card level to prevent an event, specified on the deck level by the template element, from occurring. It can only be contained in either a do or onevent element.

An example of noop is to use a <do> tag to add a "Back" link to the card. When users click on the "Back" link, generally they should be taken back to the previous card. However, the <noop> tag prevents this operation; when the user clicks on the "Back" link nothing happens.

- <**prev**> tag - The prev tag specifies navigation to the previous URL in the history.
- <**refresh**> tag - The refresh tag specifies a refresh task whereby the whatever card is being displayed will be refreshed. This task specifies the need for an update of the user agent context as specified by the contained <setvar> elements.This tag can only be nested inside an anchor, do, or onevent element. Xml:lang is not an associated attribute. User-visible side effects of the update can occur during the processing of the <refresh>.

Input Elements

- <**input**> tag supported - The input tag specifies a point where the user is prompted to enter text.

Attribute	Value	Description	Comments
name	*nmtoken*	REQUIRED. The name of the variable that is set with the result of the user's input	SUPPORTED
emptyok	true false	Sets whether the user can leave the input field blank or not. Default is "true"	SUPPORTED
format	 A a N X x M m *f nf	Sets the data format for the input field. Default is "M" A = uppercase alphabetic or punctuation characters a = lowercase alphabetic or punctuation characters N = numeric characters X = uppercase characters x = lowercase characters M = all characters m = all characters *f = Any number of characters. Replace the f with one of the letters above to specify what characters the user may enter. nf = Replace the n with a number from 1 to 9 to specify the number of characters the user may enter. Replace the f with one of the letters above to specify what characters the user can enter. The user cannot exit the input box unless the correct number or type of characters is entered. The user does not receive an error message if incorrect data is entered	SUPPORTED

Attribute	Value	Description	Comments
maxlength	*number*	Sets the maximum number of characters the user can enter in the field	SUPPORTED
size	*number_of_char*	Sets the width of the input field	NOT SUPPORTED
tabindex	*number*	Sets the tabbing position for the input field	NOT SUPPORTED
title	*cdata*	Sets a title for the input field	SUPPORTED
type	text password	Indicates the type of the input field. The default value is "text”	SUPPORTED
value	*cdata*	Sets the default value of the variable in the "name" attribute	SUPPORTED

The six display lines of the 4620 associated with feature buttons are all available for input elements. The top line of the display cannot be used for input.

The input tag causes an automatic line break before and after input text.

Only 1 input tag can exist per display line.

When a user views a page with the input tag specified, the first thing that shows up in the top line is the card title, if specified. When the user scrolls to the first line containing input, the top line shows the input box title if specified, otherwise the card title is shown. The top line displays the card title for all non-input text.

When the input box is selected, a vertical line (the "cursor") appears at the left side of the input box.

The attribute type password should only be used when it is important to not display the user’ s password on the screen. Asterisks will be displayed instead. It is also important that the password not be cached.

The phrase [enter text here] appears for all input tags if the value attribute is null. If the author specifies a non-null content in the value attribute, that content displays between brackets for that input tag.

Only the correct size, type, and number of characters are accepted in to the input box. For example, if alpha text is specified and the user types in a symbol or numeric text, the user input is not accepted. The screen repaints and the user has to re-enter their input. If the wrong kind of text is typed, the user receives an error tone. If the “n” (number) value is specified and the user types in the incorrect number of characters, their input will not be accepted.

- <**fieldset**> tag - The fieldset tag is used to group logically related elements in a card. This tag is not supported.

- <**optgroup**> tag - Sets of <optgroup> brackets can be put around <options> in a <select> list. The results in breaking a list into sublists.

Attribute	Value	Description	Comments
title	*cdata*	Sets a title for the optgroup element	SUPPORTED

- <**option**> tag - A set of option tags is needed to specify each individual item in a list. This tag must be used with the select tag.

Attribute	Value	Description	Comments
onpick	*url*	Sets what is going to happen when an user selects an item	SUPPORTED
title	*cdata*	Sets a title for the option	SUPPORTED
value	*cdata*	Sets the value to be used when setting the "name" variable in the select element	SUPPORTED

- <**select**> tag - The select tag allows for the definition of a list, embedded in a card, to allow the user to choose inputs from a list rather than having to type something in. The select tag must be used with the option tag.

Attribute	Value	Description	Comments
name	*nmtoken*	Names the variable that is set with the index result of the selection	SUPPORTED
ivalue	*cdata*	Sets the pre-selected option element. If none is specified the first item in a list is automatically selected.	SUPPORTED
multiple	true false	Sets whether multiple items can be selected. Default is "false". False is used for a single selection.	SUPPORTED
tabindex	*number*	Sets the tabbing position for the select element	NOT SUPPORTED
title	*cdata*	Sets a title for the list	SUPPORTED
value	*cdata*	Sets the default value of the variable in the "name" attribute	SUPPORTED

A single select is rendered with a small square containing a dot. A multiple select is rendered as multiple squares - blank if there is nothing in them, else a lower case “x”.

Variable Elements

- <**setvar**> tag - There are no visual rendering implications with this tag.

Attribute	Value	Description	Comments
name	*cdata*	REQUIRED. Sets the name of the variable	SUPPORTED
value	*cdata*	REQUIRED. Sets the value of the variable	SUPPORTED

- <**timer**> tag - The timer tag sets a timer that starts counting. This tag must be used with <onevent type="ontimer"> to be useful.

Attribute	Value	Description	Comments
value	*cdata*	REQUIRED. Sets the default value of the variable defined in the "name" attribute	SUPPORTED
name	*nmtoken*	REQUIRED. Names the variable that is set with the value of the timer	SUPPORTED

Character Entities

As with any syntactic language, WML has certain characters that have special meaning. The two most obvious of these characters are the < and > symbols, which surround all tags. These characters cannot be typed in directly if the designer's intent is to display these characters. Thus, all characters that can be displayed in a web browser have numeric values assigned to them. The numeric values are entered into the source web page as &#nnn; where nnn is a three-digit value. For example, the < symbol is entered as '<'.

In addition, many of these characters also have names assigned. Name values are entered into the source web page as &name; where name is the WML name associated with this character. For example, the < symbol would be entered as '<'. The set of characters defined by the World Wide Web Consortium are fully supported in the 4620 browser in conformance with the standard.

For convenience, a few of these key symbols are specified below.

Description	Symbol	Numeric Entity	Name Entity
double quotation	“	"	"
ampersand	&	&	&
apostrophe	‘	'	'
less than	<	<	

Colors and Fonts

The browser supports a 4-grayscale display. Because of the size of the screen on the 4620 IP Telephone, the browser has only a single font available for use, which is based on Latin-1. Only a normal font weight is supported. Bold, italic and different font sizes are not supported. The font used by the 4620 defines characters to have at most six pixels in width.

Wireless Telephony Applications (WTA)

Wireless Telephony Applications (WTA) are those applications designed to interact with the telephony-related functions present in a phone. The web browser supports:

- Originating a call - Click to Dial
- Adding entries to the phonebook (Add to Speed Dial entries)

The Web Browser supports the WTA application “click to dial” any link on the screen. An icon of a telephone handset is displayed to the left of a “click to dial” link when the link is initially displayed.

The Add to Phonebook WTAI function “wtai://wp/ap;” is used to add a Name and Number to the 4620 Speed Dial application. A Speed Dial icon will be displayed to the left of an “add to phonebook”. The wtai syntax is supported as a href attribute and as such any tags that support the href attribute will be able to use the “add to speed dial” function. These tags are <a>, <anchor>, <img>, <do>, <onevent>, <select>, <option>, and <optgroup>.

When a user activates the “add to speed dial” function, the web will transfer the name and number to the Speed Dial application, and the user will have the opportunity to edit the entry according to the current Speed Dial functionality.

The WTAI URI scheme is as follows:

wtai://<library>/<function> (; <parameter>)* [! <result>]

Scheme Definition:	
<>	Denotes an enumerated operator.
[]	Denotes an optional section.
I	Denotes a pair of mutually exclusive options.
( )*	Repeat none or multiple items.
*( )	Repeat one or multiple items.
library	Name that identifies the library type, WTA Public uses library "wp".
function	Function within a library, for example, "mc" for function "make call" in "wp" library.
parameter	Zero or more parameters sent to a function; should be delineated by a semicolon ";".
result	Start of result defined by "!". Optional.

Syntax Implementation

Click to Dial Functionality

To enable the click to dial functionality, use the following syntax:

wtai://wp/mc;number

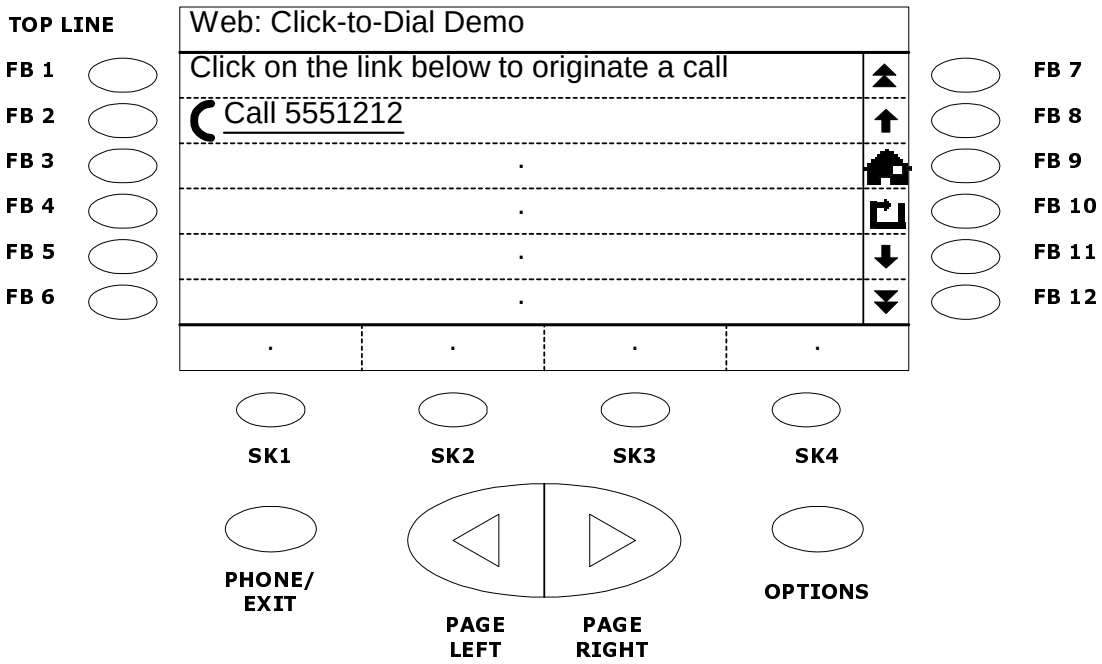
This code can be embedded into any valid WML tag that implements href or a hyperlink such as <a> tag, <anchor>, <do>, <option>, or <onevent> tags by associating these tags with a <go> tag.

Click-to-dial using <a> tag:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
        "http://www.wapforum.org/DTD/wml13.dtd">

<wml>
    <card id="callid1" title="Click-to-Dial Demo">
            <p>
                    Click on the link below to originate a call
                    <a href="wtai://wp/mc;5551212">Call 5551212</a>
            </p>
</card>
</wml>
```

The above-generated code is rendered as the following diagram:



The code shows a hyperlink as **Call 5551212** on the web screen of an Avaya 4620 IP Telephone. A phone icon precedes this hyperlink, indicating that it is a "click-to-dial" number. When this link is selected on the phone, the phone will dial the string "5551212" or any phone number followed by a semicolon in the WTAI code on the previous page.

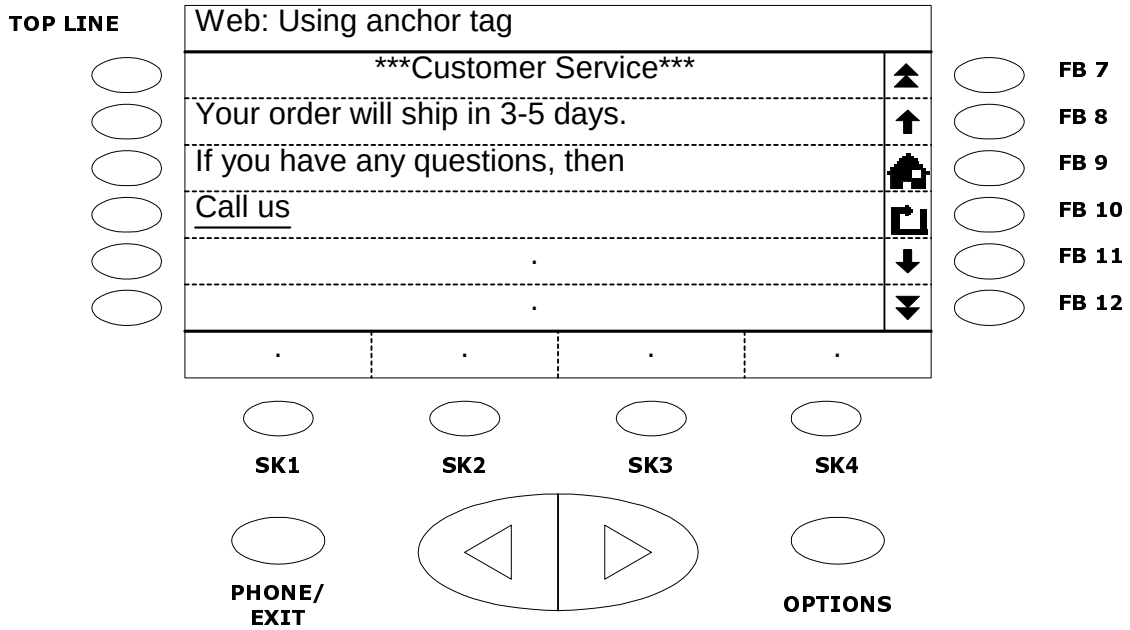
NOTE A phone icon is only generated when an <a> tag is used.

Click-to-dial using <anchor> tag:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
        "http://www.wapforum.org/DTD/wml13.dtd">

<wml>
    <card id="callid2" title="Using anchor tag">
            <p>
                    <p align="center">***Customer Service***</p>
                    Your order will ship in 3-5 days.
                    If you have any questions, then
                    <anchor>Call us
                            <go href="wtai://wp/mc;5551212"/>
                    </anchor>
            </p>
</card>
</wml>
```

The above-generated code is rendered as the following diagram:



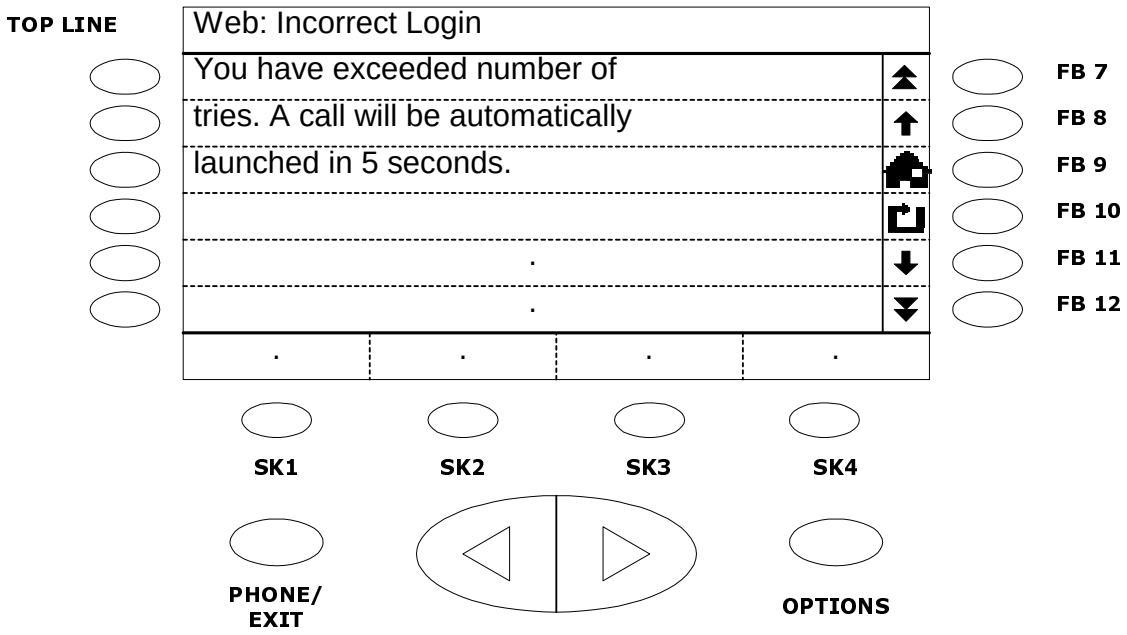
The code will show a hyperlink as **Call Us** on the web screen of an Avaya 4620 IP Telephone. When this link is selected on the phone, it will dial the string “5551212” or a number followed by a semicolon in the WTAI code on the previous page.

Click-to-dial using <onevent> tag:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
        "http://www.wapforum.org/DTD/wml13.dtd">

<wml>
    <card id="callid3" title="Incorrect Login">
            <onevent type="ontimer">
                    <timer value="50"/>
                    <go href="wtai://wp/mc;+1888 555 1212"/>
            </onevent>
            <p>
                    You have exceeded number of tries.
                    A call will be automatically launched in 5 seconds.
            </p>
</card>
</wml>
```

The above-generated code is rendered as the following diagram:



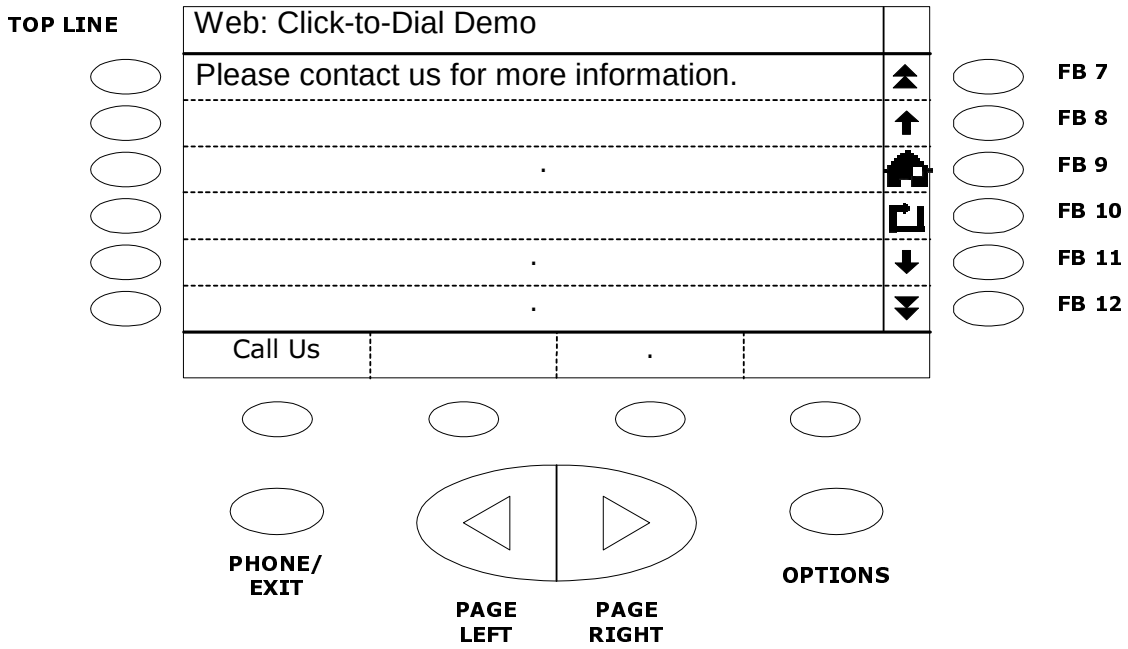
The code will automatically dial the number 1888 555 1212 after 5 seconds, once the web page is loaded.

Click-to-dial using <do> tag (softkey):

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
        "http://www.wapforum.org/DTD/wml13.dtd">

<wml>
    <card id="callid4" title="Click-to-Dial Demo">
            <p>
                    Please contact us for more information.
            </p>
            <do type="accept" label="Call Us" name="dotag1">
                    <go href="wtai://wp/mc;+18005552525"/>
            </do>
</card>
</wml>
```

The above-generated code is rendered as the following diagram:



The code will be implemented as a softkey Call Us indicating that it is a "click-to-dial" number. When this link is selected on the phone, it will dial the string "18005552525" or a number followed by a semicolon in the WTAI code above.

Add to Speed Dial Functionality

Add to Speed Dial is referred to as Add to Phone Book by WTA. When a user clicks on the add to speed dial tag, the web will transfer the name and number to the speed dial application of the Avaya 4620 IP Telephone, which will allow the user to edit and save the entry to their speed dial list.

To enable the add to speed dial functionality, use the following syntax:

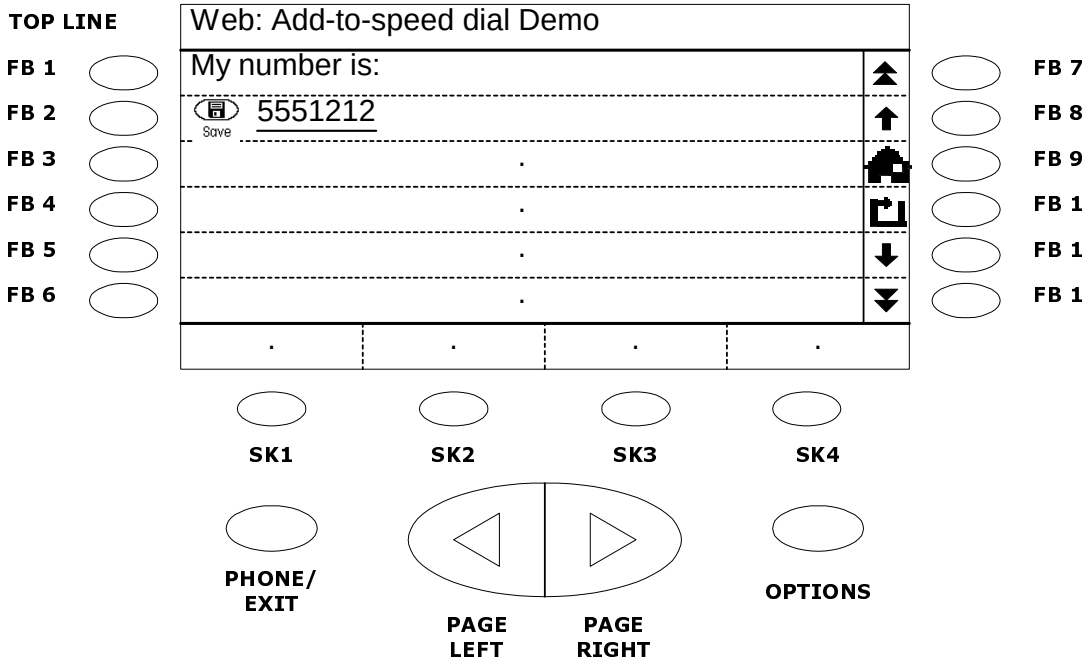
wtai://wp/ap;number;name

This code can be embedded into any valid WML tag that implements href or a hyperlink such as <a> tag, <anchor>, <do>, <option>, or <onevent> tags by associating these tags with a <go> tag.

Add to speed dial using <a> tag:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
        "http://www.wapforum.org/DTD/wml13.dtd">
<wml>
    <card id="addap1" title=”Add to speed dial Demo">
            <p>
                    My number is:
                        <a href="wtai://wp/ap;5551212;My   Company">5551212</a>
            </p>
</card>
</wml>
```

The above-generated code is rendered as the following diagram:



The code will add the entry to the speed dial group with the name "My Company" on the speed dial screen of an Avaya 4620 IP Telephone. A Save icon precedes this hyperlink, indicating that it is an "add to speed dial" number. When this link is selected on the phone, the web transfers the name and number ("My Company" and "5551212") to the telephone's speed dial application. Users can then edit and save the entry to their speed dial list.

NOTE A Save icon is generated only when an <a> tag is used.

Summary Of WML Tags And Attributes

Table 5-5. Summary Of WML Tags And Attributes

Tag	Attribute	Supported?
<a>		Yes
	accesskey	No
	href	Yes
	title	Yes
<access>		No
<anchor>		Yes
	title	Yes
<b>		No
<big>		No
 		Yes
<card>		Yes
	newcontext	No
	onenterbackward	Yes
	onenterforward	Yes
	ontimer	Yes
	ordered	No
	title	Yes

Table 5-5. Summary Of WML Tags And Attributes —*Continued*

Tag	Attribute	Supported?
<do>		Yes
	label	Yes
	name	Yes
	optional	Yes
	type	Yes, except x-*
		No
<fieldset>		No
<go>		Yes
	accept-charset	Yes
	href	Yes
	method	Yes
	sendreferer	Yes
<head>		No
<i>		No
<img>		Yes
	align	No
	alt	Yes
	height	No
	hspace	Yes
	localsrc	No
	src	Yes
	vspace	Yes
	width	No

Table 5-5. Summary Of WML Tags And Attributes —*Continued*

Tag	Attribute	Supported?
<input>		Yes
	emptyok	Yes
	format	Yes
	maxlength	Yes
	name	Yes
	size	No
	tabindex	No
	title	Yes
	type	Yes
	value	Yes
<meta>		No
<noop>		Yes
<onevent>		Yes
<optgroup>		Yes
	title	Yes
<option>		No
	onpick	Yes
	title	Yes
	value	Yes
<p>		Yes
	align	Yes
	mode	No
<postfield>		Yes
	name	Yes
	value	Yes
<prev>		Yes
<refresh>		Yes

Table 5-5. Summary Of WML Tags And Attributes —*Continued*

Tag	Attribute	Supported?
<select>		Yes
	ivalue	Yes
	multiple	Yes
	name	Yes
	tabindex	No
	title	Yes
	value	Yes
<setvar>		Yes
	name	Yes
	value	Yes
<small>		No
		No
<table>		No
<td>		No
<template>		Yes
	onenterbackward	Yes
	onenterforward	Yes
	ontimer	Yes
<timer>		Yes
	name	Yes
	value	Yes
<tr>		No
<u>		No
<wml>		Yes
{Universal Attributes}	*xml:lang*	No
	class	No
	id	Yes

Appendix D: Administering the 4620 Thin Client Directory

D

Introduction

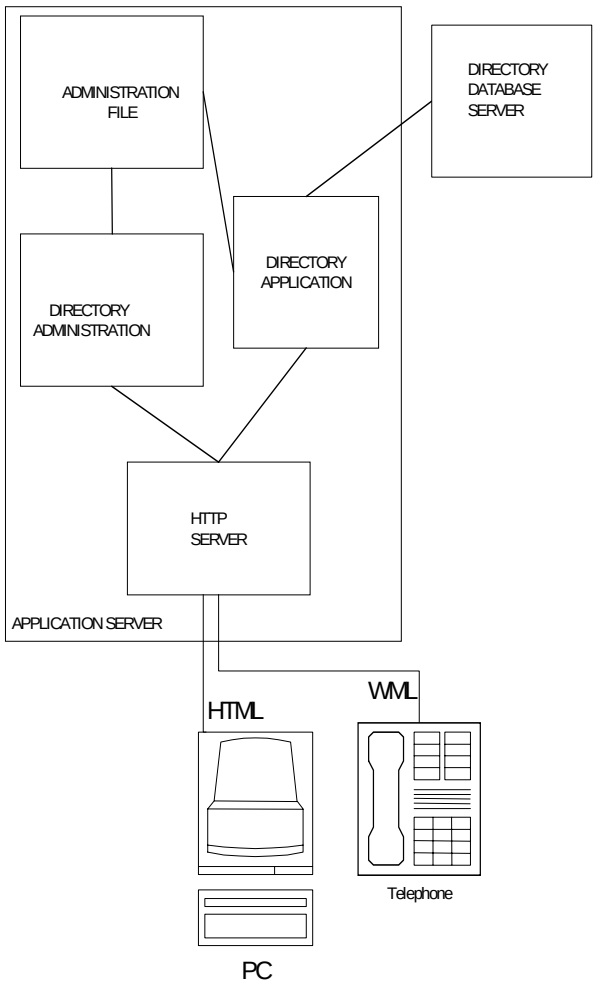
If you have a corporate database that supports the Lightweight Directory Access Protocol (LDAP), Avaya's Thin Client Directory application can communicate with that database. Your 4620 IP Telephone users can then use their phones to search for names, telephone numbers, or other information, and use the results of their searches to call a person directly, store a number on a Speed Dial button, and/or view more details about the person.

This appendix provides the information needed to install and administer Avaya's Thin Client Directory. It has four primary sections:

- Application Platform Requirements - Describes the operating environment for the Thin Client Directory application.
- Installing the Thin Client Directory on the Server - Lists the Avaya-provided download files needed for installation, pre-installation requirements, and step-by-step installation instructions.
- 4620 Web Application User Interface - Describes and illustrates the Directory application screens with which 4620 IP Telephone users perform Directory searches and review search results.
- Directory Database Administration Interface - Describes and illustrates the administration screens with which you define LDAP attributes and configure the user interface screens.

Figure D-1 on page D-2 provides a high-level overview of the Thin Client architecture.

Figure D-1. High-Level Thin Client Architecture



As shown above, the Directory application and its administration are co-resident with an HTTP server. Administration screens allow all Directory application parameters (such as the directory database server's IP address or DNS name, allowable search fields, results returned, etc.) to be set via a PC browser (web browser may be co-resident on Directory Application Server).

When a 4620 IP Telephone user initiates a directory search, the user's browser sends the search criteria to the Directory application. The Directory application sends a query (based on administered parameters) to the directory database (usually located on a separate server). The directory database server then returns search results to the Directory application, which formats them in the appropriate markup language and sends the results back to the end user. The user then has several options regarding the search results.

Application Platform Requirements

It is the LAN or System Administrator's responsibility to provide and configure the LDAP server and the operating environment on which the Thin Client Directory will be installed.

The recommended server configuration is Red Hat for Linux 8.0 (or greater) software; this version facilitates optimal, automatic Thin Client Directory application installation. Other configurations (not recommended by Avaya) require HTTP/Apache 2.0 and PHP Version 4.2.0 (with Version 4.2.4 preferred).

Installing the Thin Client Directory on the Server

Pre-Installation Requirements (Apache/PHP)

Before installing the Thin Client Directory application, the PHP Apache module (included with Red Hat 8.0) must be installed. If necessary, you can download this module for free from the http://www.php.net/downloads.php website. Go to http://www.php.net for installation instructions, otherwise, the distribution you download will contain its own set of installation instructions.

If you are not using Red Hat 8.0 or greater, Apache must be configured to accept PHP so the web server recognizes it. This process differs depending on whether PHP is being installed on Linux or Windows. Further configuration variations depend on the Apache version installed.

Avaya-Provided Download Files

Two Thin Client Directory application versions are available from the Avaya website at:

http://avaya.com/support

The recommended download version (avayadir-1.0-1.0.i386.rpm) is for Red Hat Linux 8.0 (or greater) installations only. This download allows the Red Hat Package Manager to automatically install the required directories and associated files in the correct locations.

NOTE A README file containing Thin Client Directory Application installation instructions is also available from the Avaya website, if needed.

The other version available is a Winzip-readable file, for those installations with Windows or any other operating system that are not using Red Hat for Linux 8.0 (or greater). This version requires you to select specific files to download and perform additional server/file customization to properly install the Thin Client Directory application.

The download contains these directories:

- **avayadiradmin** - Files needed for the HTML administration part of the LDAP application (including the PHP files needed for administration).
- **avayadirclient** - Files necessary for the 4620 user interface (the files that perform the search query and return search results to the telephone's display screen).
- **avayadir.ini** - Files containing settings that control the (administration and client) application. This is a protected directory that cannot be browsed. During the unzip process, it is placed in the same root as the other two sub-directories. If desired, you may move this directory outside of the HTML path, providing the new path is PHP-accessible.
- **avaydirinclude** - Common files shared between the Directory administration and client (end user) interface.
- **avayadirerror** - Text files for search-related error message generation.
- **avayadirhelp** - Text files containing end user Directory assistance.

Installing the Thin Client Directory

Installations using Red Hat for Linux 8.0 (or greater):

1. Login at the root.
2. Copy the following download file to the Linux system: **avayadir-1.0-1.0.i386.rpm**.
3. Run the following command from the command line to extract the files to the **/var/www/html/avayadir** directory: **rpm –ivh avayadir-1.0-1.0.i386.rpm**.
4. To enable password control for the Directory Administration Application, create a directory entry in the **httpd.conf** file as follows:

   NOTE The correct file name is ***httpd.conf***, not ***http.conf***.

   ```
   <Directory "/var/www/html/avayadir/avayadiradmin">
   AuthType Basic
   AuthName "Password Required"
   AuthUserFile "/var/www/password/avayadirpasswd"
   Require user ldap
   </Directory>
   ```

5. The default user/password combination is **ldap/ldap**. To change the password, run "**htpasswd /var/www/passwd/avayadirpasswd ldap**".
6. Open the file **/etc/php.ini** for editing.
7. Set the option "**short_open_tag = On**" in php.ini.

8. Uncomment the line "**extension=ldap.so**" in php.ini
9. To finish, restart the web server by running "**/sbin/service httpd restart**".
10. Now test everything out by pointing a browser at the newly created directory structure such as <http://yourserver/avayadir/avayadiradmin/index.htm>.

Installation for any other Unix-based operating system:

1. Download the winzip file and run: **unzip avayadir-1.0.zip**
2. Copy the entire tree that was created by running unzip under the documentRoot of the httpd server. For example, if your directory is /var/www/html, the directory created will be /var/www/html/avayadir.
3. Use the command "chown apache:apache /var/www/html/avayadir/avayadirini" to change the user and group of the directory /var/www/html/avayadir/avayadirini to **user:apache, group:apache**.
4. Run "**chmod 755 /var/www/avayadir/avayadirini**" to change the permission of the /var/www/html/avayadir/avayadirini to **755**.
5. To enable password control for the Directory Administration Application, create a directory entry in the httpd.conf file as follows:

   NOTE The correct file name is ***httpd.conf***, not ***http.conf***.

   ```
   <Directory "/var/www/html/avayadir/avayadiradmin">
   AuthType Basic
   AuthName "Password Required"
   AuthUserFile "/var/www/password/avayadirpasswd"
   Require user ldap
   </Directory>
   ```

6. The default user/password combination is **ldap/ldap**. To change the password, run "**htpasswd /var/www/passwd/avayadirpasswd ldap**".
7. Open the file **/etc/php.ini** for editing.
8. Set the option "**short_open_tag = On**" in php.ini.
9. Uncomment the line "**extension=ldap.so**" in php.ini
10. To finish, restart the web server by running "**/sbin/service httpd restart**".
11. Now test everything out by pointing a browser at the newly created directory structure such as <http://yourserver/avayadir/avayadiradmin/index.htm>.

Installation for Windows with Apache:

1. Extract the file **avayadir-1.0.zip** to the documentRoot folder.

   NOTE The documentRoot location will vary based on web server installation. This is the directory where the web server originates the files it serves.

2. Go to www.php.net to determine how to install and configure PHP for your server.
3. Check your web server's installation instructions to determine how to enable directory-level password control. It is *strongly recommended* that you enable password protection for the Directory administration folder **avayadiradmin**.
4. Open the file **php.ini** for editing. This file should be located in the Windows folder **c:\windows**.
5. In php.ini, set the option "**short_open_tag = On**".
6. Uncomment the line "**extension=php_ldap.dll**"
7. Save the updated **php.ini** file.
8. To finish, restart the web server.
9. Now test everything out by pointing a browser at the newly created directory structure such as: <http://yourserver/avayadir/avayadiradmin/index.htm>.

4620 Web Application User Interface

This section describes the user interface screens required for the Directory application. Because the Directory application's phone screens are accessed via the 4620's Web Access application, any Directory user interface screen you administer must use LDAP attributes only. Some examples are provided in Table D-4. Appendix C, Creating Websites for the 4620 IP Telephone provides detailed information about how web pages/screens are rendered for the 4620 IP Telephones. Once you familiarize yourself with the user interface, see Directory Database Administration Interface for instructions on completing the associated administration screens.

NOTE Because the Directory user interface screens are considered part of a web-based application, and because you may customize user interface screens, specific user instructions regarding the Directory application are not provided in the *4620 IP Telephone User's Guide.* Chapter 5, Using the Web Access Application, provides general information for working with web pages.

Generic User Interface Screen Characteristics

All Directory application phone screens have similar layouts with:

- A display area.
- Feature buttons down the left and right sides related to a text entry field or data item.
- Softkeys below the display that initiate screen-related actions, such as Search or Call.
- Web browser navigation buttons down the right side of the display, which allow the user to move forward, back and return to the Home page.

NOTE Standard softkey labels on text entry screens will be translated into the user's language, but the Directory application itself, and associated help or error messages are in English only.

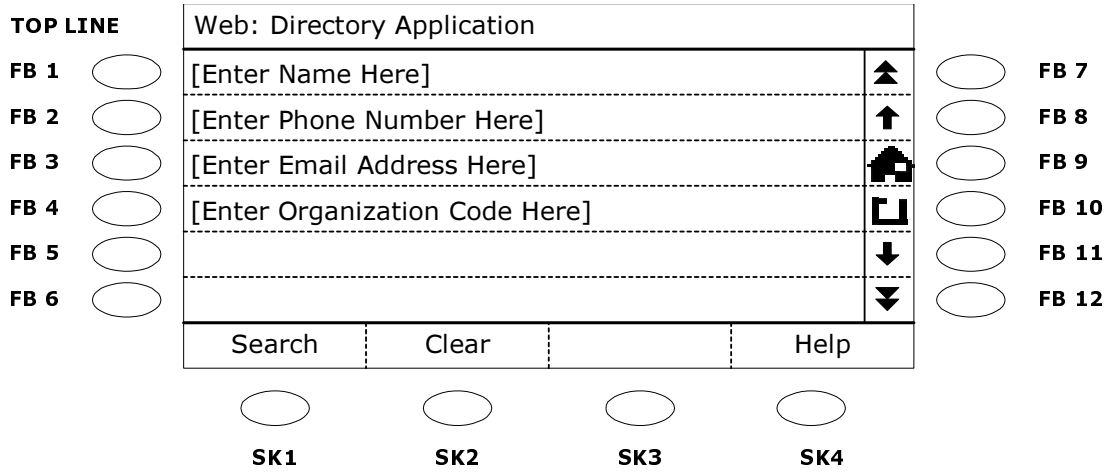
Web Application Search Screen

The Search screen displays upon user selection of the Directory application. At a minimum, two user text entry fields should be administered:

- Enter Name Here
- Enter Phone Number Here

Either field provides basic search criteria; up to four additional text entry fields may be administered.

Figure D-2. Sample Search Screen



The three softkeys at the bottom of the screen function as follows:

- **Search** - Sends user input to the Directory application to initiate a search.
- **Clear** - Discards user input.
- **Help** - Retrieves a Help page specific to the Search screen.

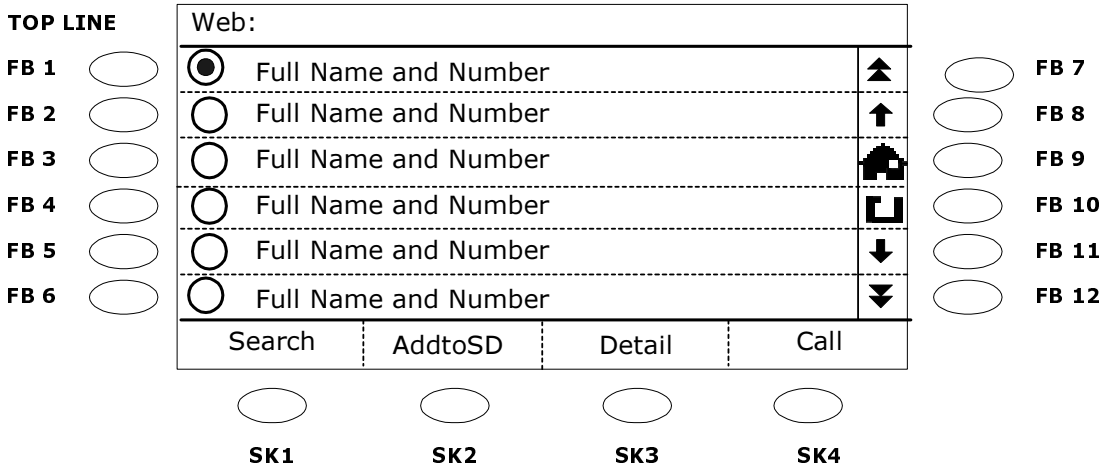
Search responses take one of two forms. A successful search (one returning at least one telephone number when a Name was provided as search criteria) displays the Successful Search screen. This screen offers options to call the number found, add it to a Speed Dial button or review more detail. An unsuccessful search (no name found, error report(s) and/or unintelligible responses) displays the Directory Trouble screen.

NOTE You administer the Search screen using the Search Administration screen, covered in Configuring the Directory Application Search Administration Screen, on page D-18.

Web Application Successful Search Screen

The Successful Search screen displays when at least one match results from a user-submitted search. The top display line provides the message “X found. Select choice.” (where X = the number of matches found) or the message “More results - please try again and refine search.” (to indicate more than 96 matches were found). The display area for this screen provides the name and phone number of up to 96 matches found by the search. The user scrolls through the matches using the web browser navigation key to move forward one page, and selects an entry by pressing the Feature button to the left of the entry.

Figure D-3. Sample Successful Search Screen



The four softkeys across the bottom of the display function as follows:

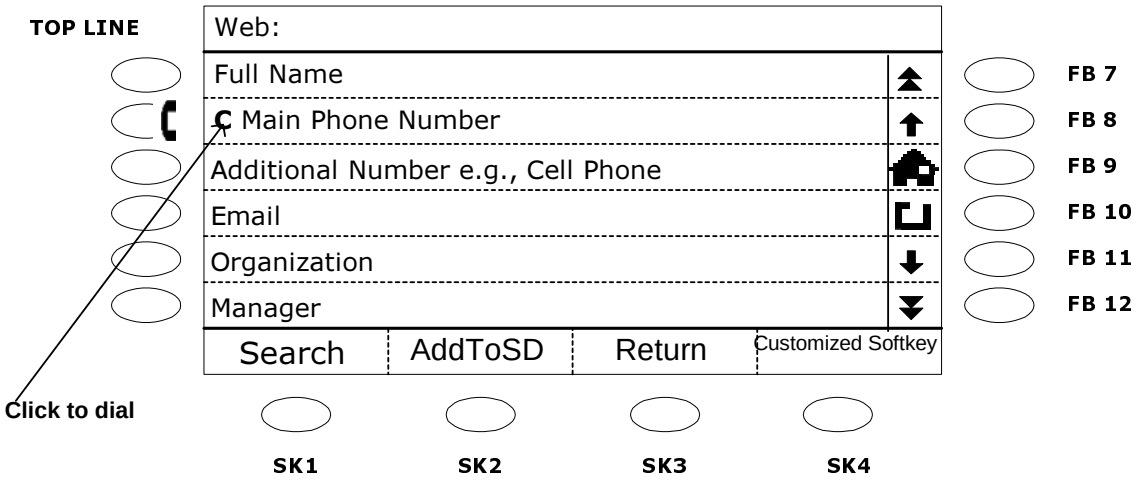
- **Search** - Displays the Search screen, to allow the user to enter new criteria and initiate another search.
- **Add to SD** - Allows the user to add a selected name and phone number to a Speed Dial button.
- **Detail** - Displays more directory information on the person selected, such as a department, secondary contact, manager, etc. (as administered). See Figure D-4 for a sample Detail screen.
- **Call** - Allows the user to initiate a call to a person listed.

Web Application Detail Screen

The Detail screen displays when a user selects the **Detail** button on the Successful Search screen. Depending on how you administer it, this screen provides additional information about the person selected on the Successful Search screen. The Full Name and Main Telephone Number of the selected person show on the first two lines as a default, but can be administered to display different data. Four additional display lines may be administered to provide specific (corporate or personal) information about the person. Examples of data you can administer to appear are shown directly below; any valid LDAP attribute can be used in their place:

- Additional Phone Number - a cell phone or other related telephone number.
- Email - the person's business email address.
- Organization - the department or organization to which this person belongs.
- Other - any other pertinent information, such as the name of the person's manager or assistant.

Figure D-4. Sample Detail Screen



A "click to dial" icon ( ) to the left of the Main Phone Number allows the user to call the person directly from the Detail screen; using this icon instead of a **Call** softkey saves a softkey for your customization. Three softkeys are labeled as follows, the fourth softkey is available for your use:

- **Search** - Displays the Search screen, to allow the user to enter new criteria and initiate another search.
- **Add to SD** - Allows the user to add a selected name and phone number to a Speed Dial button.

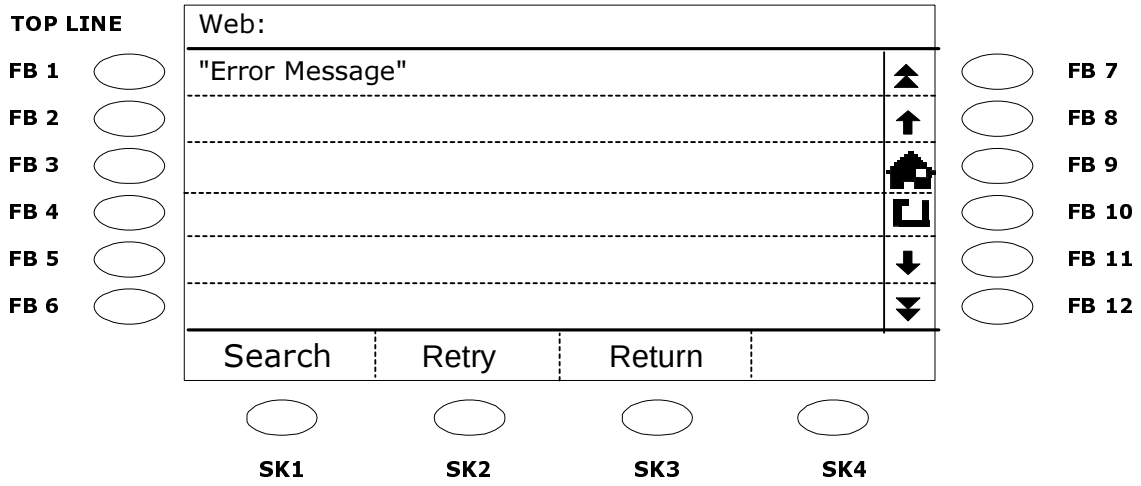
- **Return** - Displays the Search screen, including the Name field entered by the user to initiate the most recent search.

NOTE You administer the Detail screen using the Details Administration screen, covered in Configuring the Directory Application Details Administration Screen, on page D-20.

Web Application Directory Trouble Screen

Unsuccessful Directory searches can occur for several reasons, from an inability to connect to the server for a search, to finding no Directory listings matching the search criteria. Any search-related problem displays as an error message on the Directory Trouble screen, shown below in Figure D-5.

Figure D-5. Sample Directory Trouble Screen



The Trouble Screen's softkeys function as follows:

- **Search** - Displays the Search screen, to allow the user to enter new criteria and initiate another search.
- **Retry** - Allows the user to re-initiate the search using the same search criteria.
- **Return** - Displays the Search screen, with the Name field entered by the user to initiate the most recent search.

Possible reasons for search failure and the resulting messages displayed on the Trouble screen follow in Table D-1.

Table D-1. Search Failure Causes and Corresponding Trouble Screen Error Messages

Cause of Search Failure	LDAP Result Code	Trouble Screen Message
N/A. The corresponding LDAP Result Code represents a successful search.	0	No message displayed; search was successful.
Operations/Protocol error	1,2	Operations/Protocol error.
Server-generated time-out	3	Server timed out.
More than 96 entries match the Search criteria	4	Size limit exceeded.
Various unexpected errors. (These result codes should never be received).	5, 6, 10, 11, 12, 13, 14, 18, 19, 20, 21, 34, 36, 54, 64, 65, 66, 67, 68, 69, 71	Invalid response.
Authentication not accepted	7, 8, 48, 49, 50, 53	Authentication error.
Telephone Number not recognized	16, 17	Telephone Number not recognized.
Object not found	32	No results found.
Server responds with "null" as data	N/A	No results found.
Server not available	51, 52	Server not available.
Other, unspecified	80	An unknown problem has occurred.
If any of these system values are null (except DIRUSERID and DIRSRVRPWD, which are optional and hence may remain null), and the user tries to access the Directory Application, the Trouble Screen is presented to the user.	N/A	Insufficient Administrative Information.
The directory server does not respond at all within an administrable amount of seconds (default is 10 seconds)	N/A	Unable to contact server.

Table D-1. Search Failure Causes and Corresponding Trouble Screen Error Messages—*Continued*

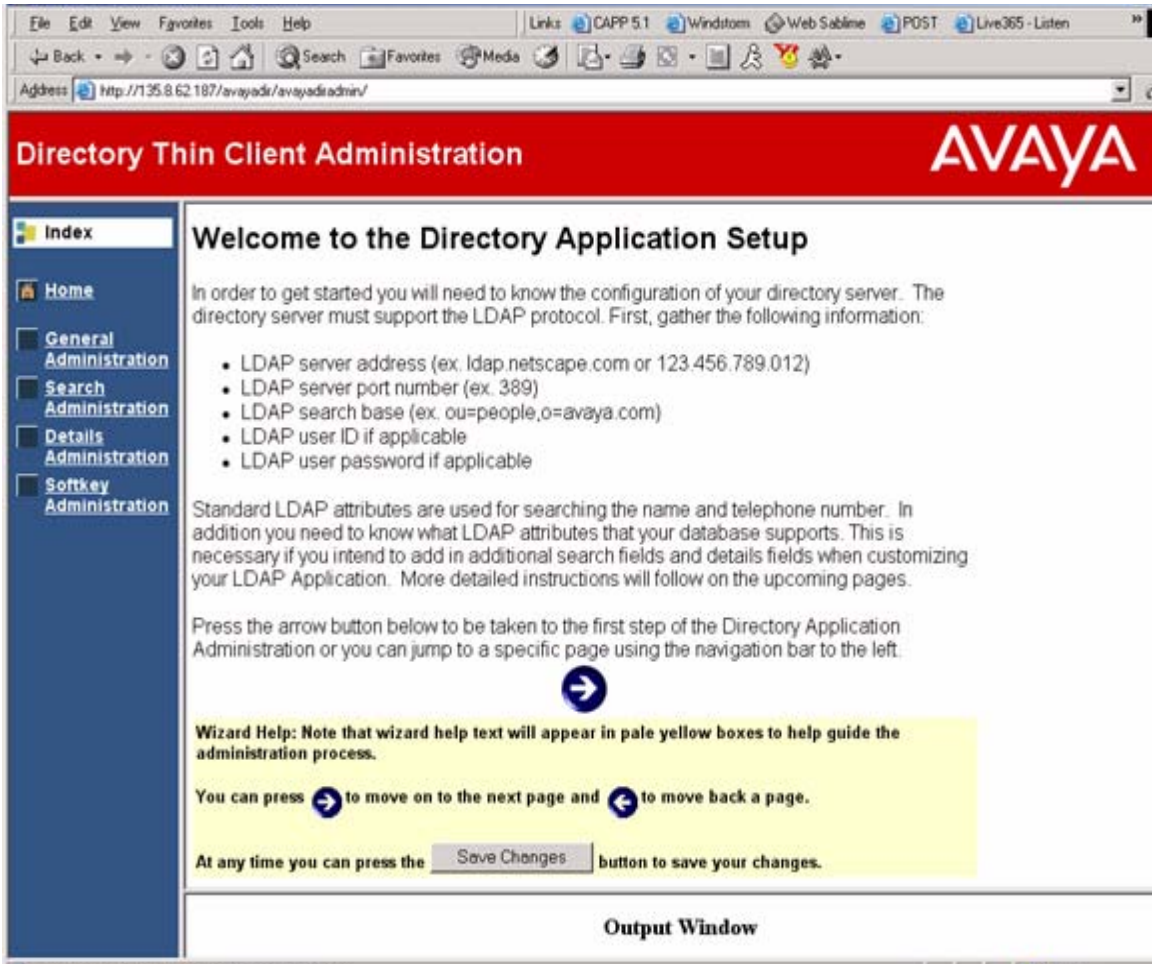
Cause of Search Failure	LDAP Result Code	Trouble Screen Message
When the Directory Application receives a request for a Search screen, it will send a Search screen in response only if the minimum administrative information has been supplied. Otherwise, a Trouble Screen will be sent to the endpoint.	N/A	Insufficient Administrative Information.
When the Directory Application receives a request for a search from an endpoint, it will initiate a connection to the directory database server and, if successful, it will format and send a query to the database server based on the input received from the endpoint. If the input received from the endpoint is null, a Screen will be sent to the endpoint.	N/A	Insufficient Query Information.
If a connection to the database server cannot be established, or if the connection fails before a response is received, a Trouble Screen will be sent to the endpoint.	N/A	Connection Failure.
When the Directory Application receives a successful response from the database server, it sends a Successful Result screen to the endpoint. If no matching database entries are returned, it sends a No Match Result screen to the endpoint. If an error is returned by the database, a Trouble screen is sent to the endpoint.	N/A	No Match Result.
Cannot be determined	9, 22 - 31, 35, 37 - 47, 55 - 63, 70, 72 - 79, and 81 - 90	Unknown Error.

Directory Database Administration Interface

The Directory application file you download from the Avaya website contains five primary screens on which you administer and customize the Thin Client Directory. Additionally, each administration screen has embedded Help to guide you through the administrative process. The primary screens are:

1. **Welcome screen** - The Home Page for administering your Directory application. This screen provides pre-administration requirements, basic administration information, links to all other administration screens, and a link to administrative Help.

Figure D-6. Welcome Screen


File Edit View Favorites Tools Help
Links CAPP 5.1 Windstorm Web Sublime POST Live365 - Listen
Back Search Favorites Media
Address http://135.8.62.187/avayadir/avayadiradmin/
Directory Thin Client Administration
AVAYA
Index
Home
General Administration
Search Administration
Details Administration
Softkey Administration
Welcome to the Directory Application Setup
In order to get started you will need to know the configuration of your directory server. The directory server must support the LDAP protocol. First, gather the following information:
LDAP server address (ex. ldap.netscape.com or 123.456.789.012)
LDAP server port number (ex. 389)
LDAP search base (ex. ou=people,o=avaya.com)
LDAP user ID if applicable
LDAP user password if applicable
Standard LDAP attributes are used for searching the name and telephone number. In addition you need to know what LDAP attributes that your database supports. This is necessary if you intend to add in additional search fields and details fields when customizing your LDAP Application. More detailed instructions will follow on the upcoming pages.
Press the arrow button below to be taken to the first step of the Directory Application Administration or you can jump to a specific page using the navigation bar to the left.
Wizard Help: Note that wizard help text will appear in pale yellow boxes to help guide the administration process.
You can press to move on to the next page and to move back a page.
At any time you can press the Save Changes button to save your changes.
Output Window

NOTE The Welcome screen (Home page) provides a checklist of the values required to set up general administration, such as the LDAP Server Address. Be sure you have this required information before beginning to configure the General Directory Application Administration screen.

2. **General Directory Application Administration screen** - You provide general information about your Directory application, such as the Application Title displayed at the top of the first user interface screen, the LDAP Server Address, the search root and port network identification, optional User ID and Password for accessing the application, and the amount of time to be allowed for a search.
3. **Directory Application Search Administration screens** - You specify required (and optional) LDAP search attributes that display on the (user interface) Search screen.
4. **Details Administration screen** - You specify the detail information the user sees on the (user interface) Detail screen, such as an alternate phone number for a person found, the person's email address, etc.
5. **Softkey Administration screen** - Allows you to (optionally) specify additional softkeys, to appear below the (user interface) Detail screen's display area.

NOTE The Directory Application administration interface is in the English language only.

Each screen has required and optional parameters. The input fields have a definition and/or explanation of what is required to their right in the yellow areas. There may also be yellow Help areas at the bottom of a screen to help you populate the screens correctly. You can select the **Home** option from the left side of any administration screen to return to the Welcome screen (Home page).

The bottom of each screen provides navigation and save options, as illustrated below:

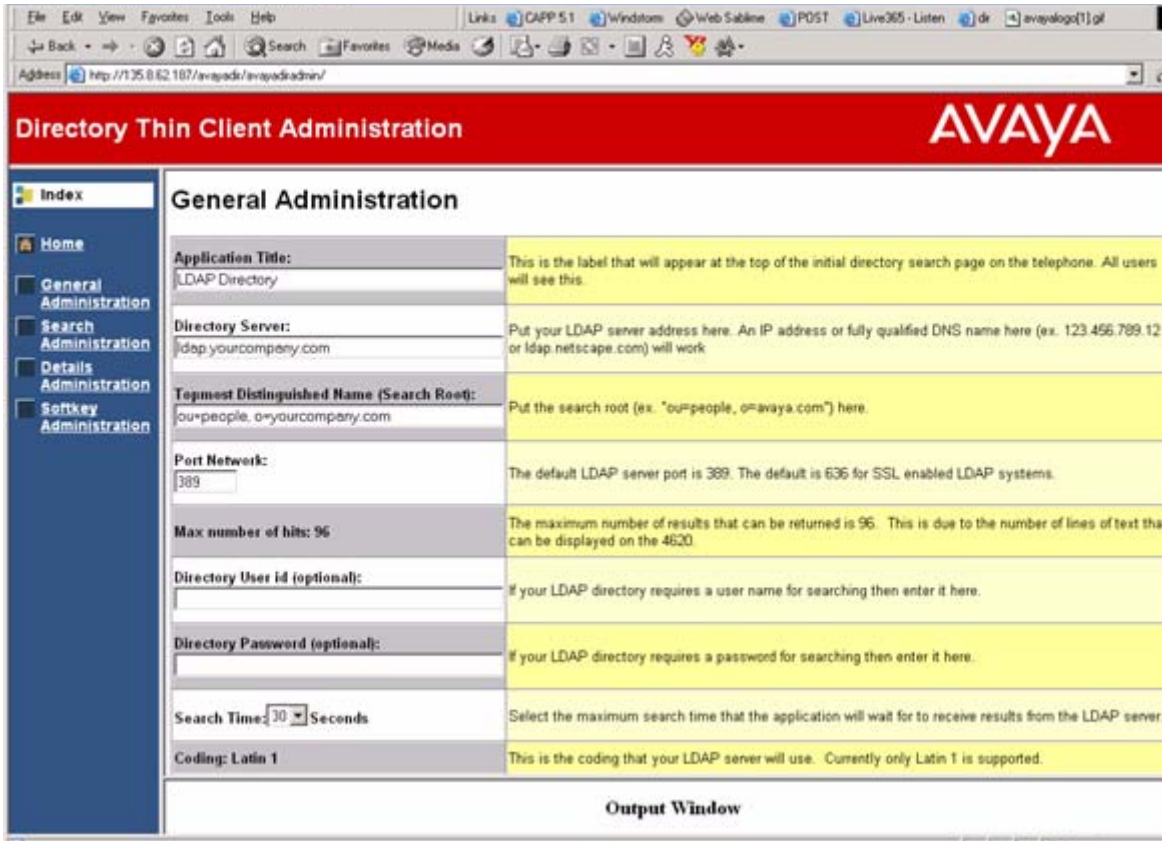
After entering the values for a screen, press the **Save Changes** button to save your entries, then use the **Right Arrow** or **Left Arrow** buttons to move from that screen to another. Pressing an arrow button without first saving what you entered or changed causes a dialog box to display. The dialog box lets you confirm that you do not want to retain your entries (or any changes you've made to existing values) or allows you to select **Cancel** to return to the screen and save the data.

Configuring the required information in accordance with the instructions in this section allows the Thin Client Directory application to communicate properly with the LDAP server. After configuring and saving the required information, test the Directory application to be sure the user interface screen values are correct, that the application is interfacing properly with the LDAP server, and that the Directory Application server is interfacing properly with the end user's phone.

Configuring the General Directory Application Administration Screen

1. From the Welcome screen, select the **General Administration** screen link (or select the **Right Arrow** icon at the bottom of the Welcome screen).

Figure D-7. Directory Application Administration Screen


Directory Thin Client Administration
AVAYA
Index
Home
General Administration
Search Administration
Details Administration
Softkey Administration
General Administration
Application Title:
LDAP Directory
This is the label that will appear at the top of the initial directory search page on the telephone. All users will see this.
Directory Server:
ldap.yourcompany.com
Put your LDAP server address here. An IP address or fully qualified DNS name here (ex. 123.456.789.12 or ldap.netscape.com) will work
Topmost Distinguished Name (Search Root):
ou=people, o=yourcompany.com
Put the search root (ex. "ou=people, o=avaya.com") here.
Port Network:
389
The default LDAP server port is 389. The default is 636 for SSL enabled LDAP systems.
Max number of hits: 96
The maximum number of results that can be returned is 96. This is due to the number of lines of text that can be displayed on the 4620.
Directory User id (optional):
If your LDAP directory requires a user name for searching then enter it here.
Directory Password (optional):
If your LDAP directory requires a password for searching then enter it here.
Search Time: 30 Seconds
Select the maximum search time that the application will wait for to receive results from the LDAP server
Coding: Latin 1
This is the coding that your LDAP server will use. Currently only Latin 1 is supported.
Output Window

2. All fields except Directory User ID and Directory Password are required. Table D-2 shows the Administration screen fields, their associated key names, default values, and descriptions:

Table D-2. Administration Screen Fields

Field Title	Key Name	Default	Description
Application Title	DIRSVRNAME	4620 Directory Application	Label appearing at top of the user interface's Directory Search screen.
Directory Server	DIRSRVR	Null	LDAP server address, IP address or fully-qualified DNS name.
Topmost Distinguished Name (Search Root)	DIRTOPDN	Null	The search root base (usually "ou=people" or o=company name). Note that spaces and other special characters may need to be treated as specified in RFC 2253, *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*.
Port Network	DIRLDAPPORT	389 for LDAP 686 for SSI-enabled LDAP	Directory Server Port.
Max number of hits		96	The maximum number of result entries that can be displayed on the 4620.
Directory User ID	DIRUSERID	Optional	User name for authorized Directory search, if required.
Directory Password	DIRSRVRPWD	Optional	User's password for authorized Directory search, if required.
Directory Search Time	DIRSEARCHTIME	10 seconds	Maximum amount of time the application will wait for search results (01 - 59 seconds).
Directory Coding	DIRCODING	Latin 1	No other option is currently available.

3. Press the **Save Changes** button as stated at the bottom of the screen to save the values entered. When you complete the final administration screen, you will have the opportunity to review all values on all screens.

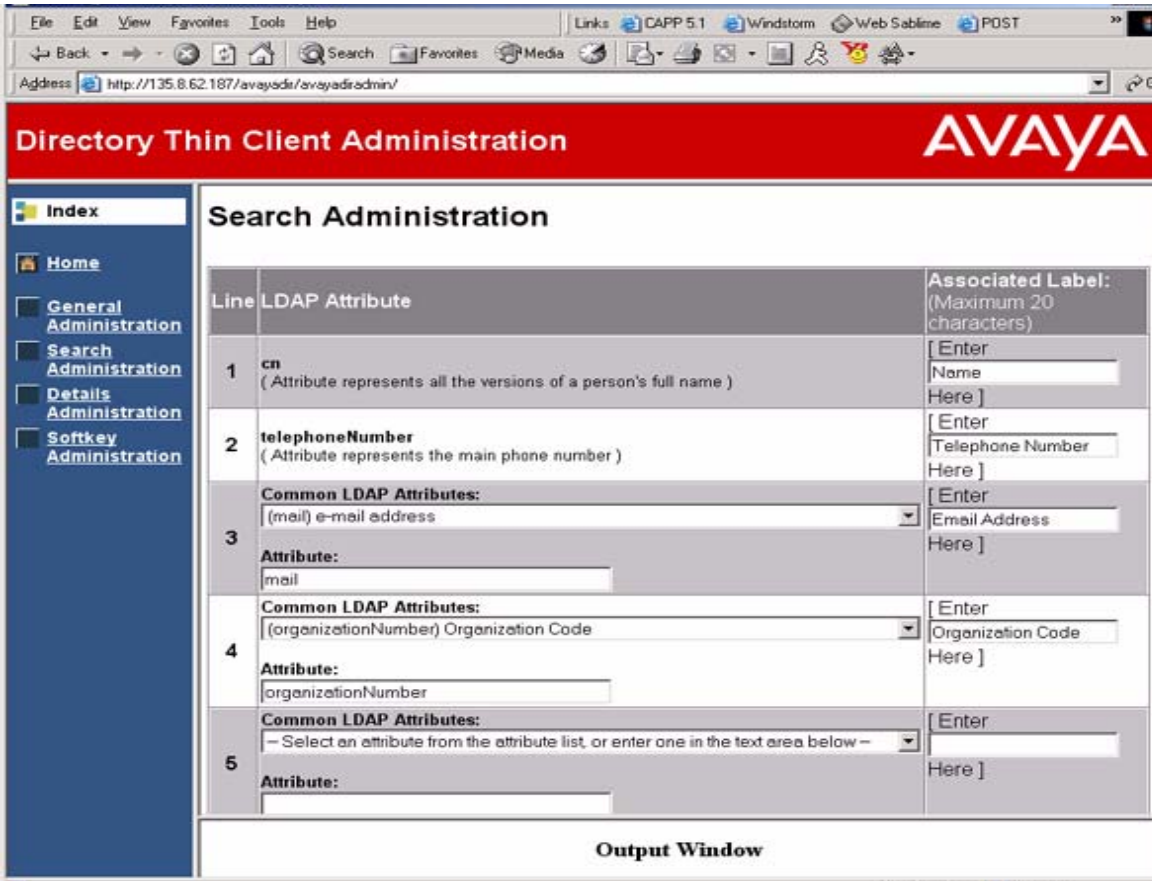
Configuring the Directory Application Search Administration Screen

The Search screen's administration requires you to provide labels for the LDAP attributes that appear on the user interface Search screen; these are the labeled search fields the end user sees when the Search screen displays.

Any Customer-Defined Label you create populates the *Label* value of the "Enter *Label* Here" text entry box on the Search Administration screen. This label also displays as the text entry prompt on the user interface Search screen. See Figure D-2 on page D-8 for an illustration of the user interface Search screen

1. From the Welcome screen, select the **Search Administration** screen link (or select the **Right Arrow** icon at the bottom of the General Administration screen).

Figure D-8. Search Administration Screen



2. Enter the search fields, corresponding LDAP attribute names, and associated labels by which your 4620 end users will search your corporate Directory. The Search Administration screen contains the fields shown in Table D-3.

Table D-3. Search Administration Screen Fields

Search Screen Line #	Search Field/ Search Object	LDAP Attribute Name	Associated (Customer-Defined) Label (20 characters maximum)
1	Name (fixed)	cn	Customer administrable.
2	Main Phone Number (fixed)	phoneNumber	Customer administrable.
3	Email (default)	mail	Customer administrable.
4	Customer administrable	Customer administrable	Customer administrable.
5	Customer administrable	Customer administrable	Customer administrable.
6	Customer administrable	Customer administrable	Customer administrable.

Example: Line 3 above shows a search field “Email” with the LDAP attribute “mail.” If you enter the Associated Label (column 4) as “Email Address” the 4620 users’ Search screen third line prompts them to “Enter Email Address Here”.

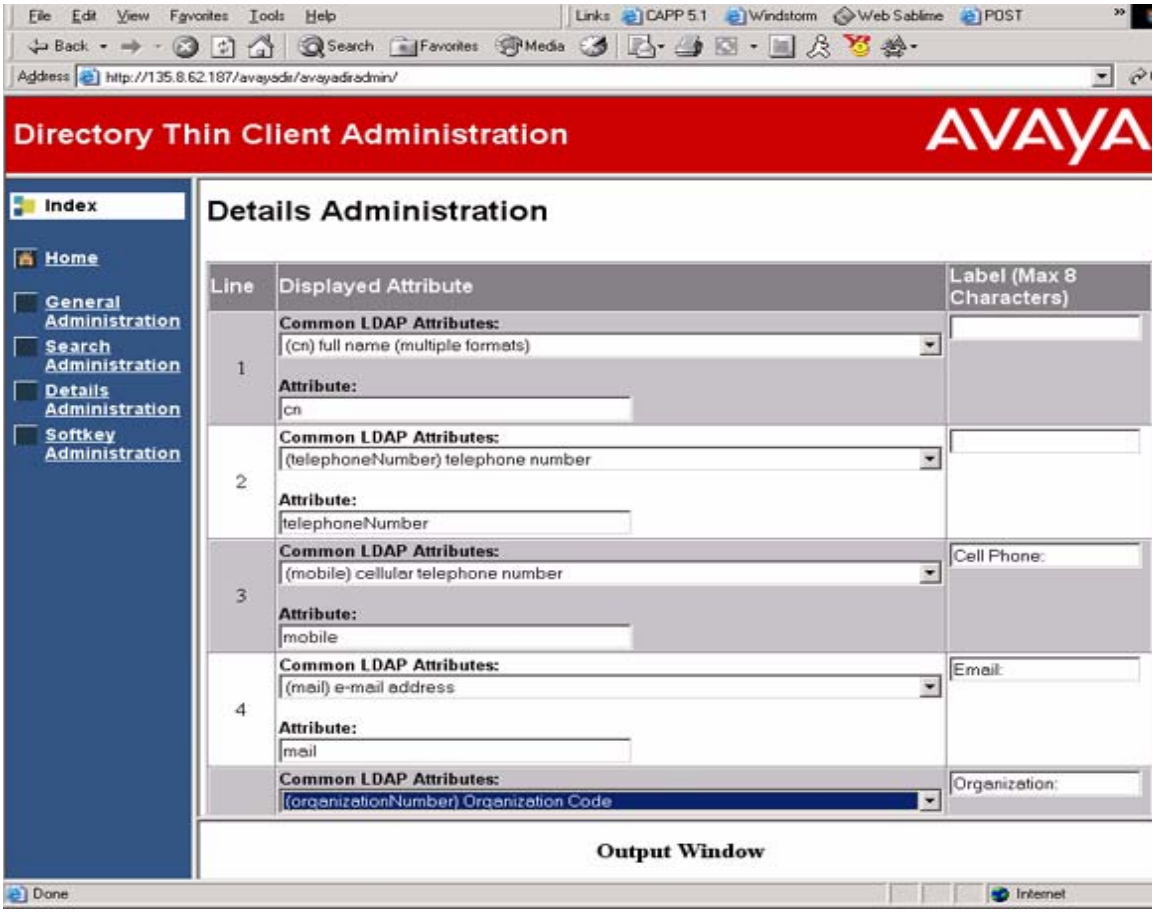
You can populate fields with well-known LDAP attributes from an Avaya-provided drop-down list. Table D-4, on page D-23 provides a list of allowable attributes you can use to label such fields.

Configuring the Directory Application Details Administration Screen

The Detail screen's administration requires you to provide the LDAP attributes that will appear on the user interface Details screen; these are the details the end user sees about a selected person when the Details screen displays.

1. From the Welcome screen, select the **Details Administration** screen link (or select the **Right Arrow** icon at the bottom of the Search Administration screen).

Figure D-9. Details Administration Screen



2. Enter the LDAP attribute names representing the detail information you want to display about a person found by a search. These entries appear to your 4620 end users on the user interface Detail screen, as illustrated in Web Application Detail Screen, on page D-10.

NOTES
- It is assumed that a minimum of name and telephone number will be shown as detail information, but you can change these defaults and provide different attributes, if desired.
- To override an attribute that does not appear in a drop-down list, change the **Use Other** radio box next to the appropriate Displayed Attribute from “Yes” to “No” then enter the custom attribute in the **Other** text entry field.
- Labels are not required because the detail attribute should be unique enough for end user identification. If you feel the attribute does not provide a sufficient description, you may include a label of up to 8 or less characters, with the understanding that the number of characters in the text display area will be reduced accordingly.

You can populate LDAP attributes from an Avaya-provided drop-down list. Table D-4, on page D-23 provides a list of allowable attributes you can use to label such fields.

Configuring the Directory Application Softkey Administration Screen

Avaya provides specific softkeys with specific functions on each user interface screen. Where space is available in the softkey area at the bottom of a (user interface) screen, you may optionally configure up to five additional softkeys and link them to specific Detail screen display fields. For example, you may have configured “Manager” as a detail screen attribute, which would show a [found] person’s manager as part of the detail information. Linking a softkey to that field can provide a report/list of *any* person in the directory who has that specific manager as part of his or her own detail information.

The Softkey Administration screen lists all attributes you previously defined on the Detail Administration screen as “From” attributes. You configure softkeys by providing a “To” attribute that establishes a link between the two attributes, and which is used as the softkey’s label. You can populate LDAP “To” attributes using an Avaya-provided drop-down list as shown in Table D-4, on page D-23. You may also provide a specific label for the new softkey, using the minimal number of characters that will display in the screen’s softkey label area.

Figure D-10. Softkey Administration Screen

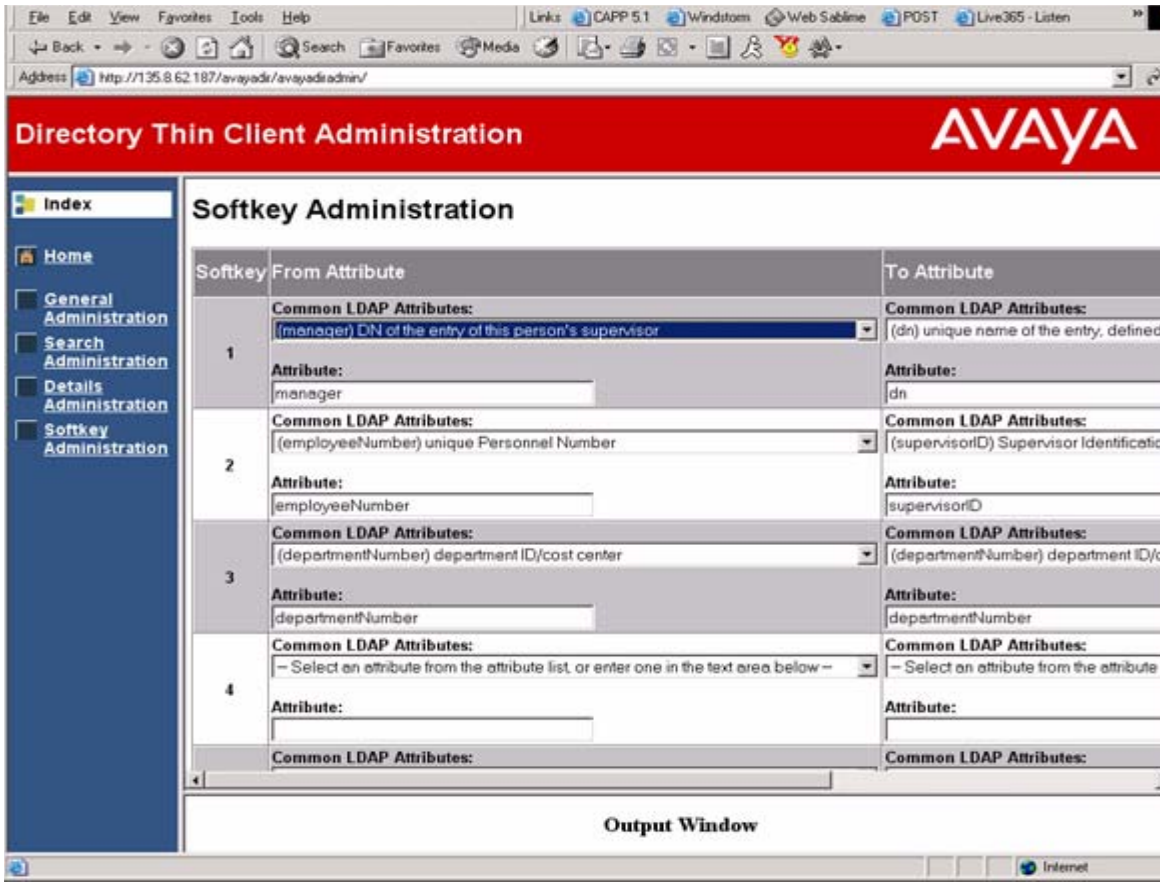


Table D-4. List of Drop-Down Attributes available for Search, Query and Details Administration Screens

Field	LDAP Attribute
person	sn cn userPassword telephoneNumber description
organizationalPerson	title registered address telexNumber teletexTerminalIdentifier telephoneNumber internationalISDNNumber facsimileTelephoneNumber street postOfficeBox postalCode postalAddress physicalDelieveryOfficeName ou st l
inetOrgPerson	businessCategory carLicense departmentNumber employeeNumber employeeType givenName homePhone homePostalAddress initials labeledURL mail manager mobile pager roomNumber secretary uid userCertificate;binary x500uniqueIdentifier

Index

Numerics

4600 Series IP Telephone
  Restart 5-9
4600 Series IP Telephone Customizable System Parameters 4-29
4600 Series IP Telephone Scripts and Application Files 4-19
4600 Series IP Telephones 2-7
  Administering on Avaya Media Servers 4-4
  Administering Options for 4-28
  Administration Alternatives and Options 4-2
  DHCP and TFTP Servers 2-8
  DNS Addressing 4-31
  Dual Connection Architecture 2-7
  Initialization Process 2-9
  Network Audio Quality Display 4-25
  Registration and Authentication 2-8
  Single Connection Architecture 2-7
  Software 2-8
  WAN Considerations 2-8
4620 Backup/Restore 4-41
4620 IP Telephone
  Creating Websites for C-1
  Customizable System Parameters 4-39
  Customizing the 4-39
4620 IP Telephone Customizable System Parameters 4-39
4620 Thin Client Directory, Administering the D-1
4620 Web Application User Interface D-7
4630/4630SW Backup/Restore 4-36
4630/4630SW Call Log Archive 4-38
4630/4630SW Customizable System Parameters 4-34
4630/4630SW IP Telephone, Creating Websites for B-1
4630/4630SW IP Telephone, customizing 4-33
46xx IP Telephone MIB A-1

A

About This Guide 1-1
Add-to-Speed Dial Functionality, for WTA Applications C-23
Administering 4600 Series IP Telephones on DEFINITY/MultiVantage Servers 4-4
Administering DHCP and TFTP Servers 4-5
Administering Options for the 4600 Series IP Telephones 4-28
Administering the 4620 Thin Client Directory D-1
Administration Alternatives and Options for 4600 Series IP Telephones 4-2
Application Files, and Scripts for 4600 Series IP Telephones 4-19
Architecture
  Dual Connection 2-7
  Single Connection 2-7
Avaya - 46xx IP Telephone MIB A-1
Avaya TFTP (Suite Pro) 4-18

B

Backup/Restore for 4620 IP Telephone 4-41
Backup/Restore, for 4630/4630SW 4-36

C

Call Log Archive, for 4630/4630SW 4-38
Click to Dial Functionality, for WTA Applications C-19
Configuration and Installation, Suggestions for 2-6
Conventions Used in This Guide 1-4
Creating Websites for the 4620 IP Telephone C-1
  Anchor Elements C-6
  Character Entities C-16
  Colors and Fonts C-17
  Event Elements C-8
  General Background C-2
  Image Elements C-7
  Input Elements C-13
  Summary Of WML Tags And Attributes C-24
  Task Elements C-12
  Text Elements C-5
  Text Formatting Tags C-5
  Variable Elements C-16
  WML Document Skeleton C-2
Creating Websites for the 4630/4630SW IP Telephone B-1
  Browser Features and Behavior B-2
  Design Guidelines B-10
  General Background B-2
Customer Support 1-8
Customizing System Parameters for 4600 Series IP Telephones 4-29
Customizing System Parameters for 4620 IP Telephone 4-39
Customizing System Parameters for 4630/4630SW IP Telephones 4-34
Customizing the 4620 IP Telephone 4-39
Customizing the 4630/4630SW IP Telephone 4-33

Customizing the Site-Specific Option Number (SSON) 4-31

D

DEFINITY Releases 9, 9.5, and 10 4-4
Delay and Jitter 2-2
DHCP 2-3
DHCP and TFTP Server Administration 4-5
DHCP and TFTP Servers, for 4600 Series IP Telephones 2-8
DHCP and VoIP 2-3
DHCP Configuration, Choosing 4-6
DHCP Generic Setup 4-7
DHCP Server 2-8
DHCP Server Setup 4-6
DHCP Server, Windows 2000 Setup 4-14
DHCP Server, Windows NT 4.0 Setup 4-9
DHCP Software Alternatives 4-7
Directory Database Administration Interface D-14
DNS Addressing 4-31
Document Change History 1-2
Document Organization 1-2
Dual Connection Architecture 2-7

E

Enhanced Dialing Procedures, for 4620 IP Telephone 4-32
Enhanced Local Dialing 4-32
Error Conditions 5-1
Error Messages 5-12

H

H.323 Standard 2-3
Hardware Requirements 3-1

I

IETF Documents 1-6
Initialization Process, for 4600 Series IP Telephones 2-9
Installation and Configuration, Suggestions for 2-6
Installation, Network Information Required before installing 4-6
Installing the Thin Client Directory on the Server D-3
Intended Audience 1-1
IP Address Lists and Station Number Portability 2-6
ISO/IEC, ANSI/IEEE Documents 1-8
ITU Documents 1-8

M

MIB, for 46XX IP Telephones A-1
MultiVantage Release 1.1 4-4

N

NAT 2-4
Network Assessment and VoIP 2-5
Network Audio Quality Display, on 4600 Series IP Telephones 4-25
Network Information Required Before Installation 4-6
Network Information, Required 4-5

O

Online Documentation 1-4
Options, entering via the Telephone Dialpad 4-32
Options, for 4600 Series IP Telephone Administration 4-2
Overview of Voice over IP (VoIP) 2-1

Q

QoS 2-4, 4-23
  DIFFSERV 4-24
  IEEE 802.1D and 802.1Q 4-23
  RSVP and RTCP 4-27
  UDP Port Selection 4-25
QoS and VoIP 2-4
QoS, and 4600 Series IP Telephones 4-23

R

Registration and Authentication, of 4600 Series IP Telephones 2-8
Related Documents 1-5
Reliability and Performance 2-6
Requirements 3-1
  Hardware 3-1
  Software 3-4
Reset Administrative Option 5-8
Restart the Telephone 5-9
RSVP and RTCP 4-27

S

Scripts and Application Files, for 4600 Series IP Telephones 4-19
Security 2-7
Single Connection Architecture 2-7
Site-Specific Option Number, customizing 4-31
SNMP 2-4
SNMP and VoIP 2-4
Software Alternatives, for DHCP 4-7
Software Checklist 4-5

Software Requirements 3-4
Software, for 4600 Series IP Telephones 2-8
Syntax Implementation, for WTA Applications C-19
System Values, Reset 5-8
System Values, Resetting 5-8

T

Tandem Coding 2-2
Terms Used in This Guide 1-3
TFTP 2-3, 4-17
TFTP (Suite Pro), Avaya 4-18
TFTP and DHCP Server Administration 4-5
TFTP and VoIP 2-3
TFTP Generic Setup 4-18
TFTP Server 2-8
TFTP Server Setup 4-17
TFTP Settings File, contents of 4-22
Thin Client Directory, Administering the D-3
Troubleshooting
  Parameter Values 5-11
Troubleshooting Guidelines 5-1

U

Upgrade Script, contents of 4-21

V

View Administrative Option 5-10
VLAN Considerations 4-27
Voice over IP. See VoIP 2-1
VoIP 2-1
  Delay and Jitter 2-2
  DHCP 2-3
  H.323 Standard 2-3
  IP Address Lists and Station Number Portability 2-6
  NAT 2-4
  Network Assessment 2-5
  Overview, Voice over IP 2-1
  QoS 2-4
  Reliability and Performance 2-6
  Security 2-7
  SNMP 2-4
  Tandem Coding 2-2

W

WAN Considerations, for 4600 Series IP Telephones 2-8
Wireless Telephony Applications (WTA) C-17